اُردو زَبان میں اِنفارمیشن ٹیکنالوجی کا وَاحِد مُستند جریدہ

اگست 2014

قیمت 65 روپے

پوسٹل رجسٹریشن نمبر
MC-1264

فہرست

8 صفحات پر مشتمل خصوصی مفت ڈاؤن لوڈز

صفحہ نمبر:36

مستقل سلسلے

سرپرستِ اعلیٰ

گوہر رحمن

چیف ایڈیٹر

امانت علی گوہر

ایڈیٹر

علمدار حسین

اسسٹنٹ ایڈیٹر

رانا محمد امین اکبر

مشاورت

شبیر حسین قریشی، محبوب الٰہی مخمور

قیمت شمارہ: 65 روپے

سالانہ خریداری برائے پاکستان

800 روپے

سالانہ خریداری برائے بیرونِ ممالک

500 + پوسٹیج کے اخراجات

خط وکتابت کا پتا

پی او باکس نمبر 786، کراچی 74200

ٹیلی فون نمبرز

021-36990987

0342-2507857

0313-6090662

ویب سائٹ

www.computingpk.com

ای میل ایڈریس

editors@computingpk.com

آئی ایس ایس این نمبر

1993-2952

پوسٹل رجسٹریشن نمبر

MC-1264

سال بھر حاصل کرنا بے حد آسان......!!

آئی ٹی کی دنیا کا منفرد اور آپ کا پسندیدہ میگزین "کمپیوٹنگ" پاکستان بھر میں دستیاب ہے۔ لیکن آپ سالانہ خریدار بن کر حاصل کرسکتے ہیں زبردست فائدہ

بنیے سالانہ خریدار صرف 800 روپے میں......!!

یعنی کمپیوٹنگ کے تمام شمارے حاصل کرسکتے ہیں گھر بیٹھے بذریعہ رجسٹرڈ ڈاک۔

ساتھ ہی حاصل کرسکتے ہیں ایک درجن سے زائد پرانے شماروں کی سافٹ کاپیز بالکل مفت

سالانہ خریداری حاصل کرنے کا طریقہ

سالانہ خریداری حاصل کرنا بے حد آسان ہے۔ آپ ماہنامہ کمپیوٹنگ کے پتے پر مبلغ آٹھ سو روپے کا منی آرڈر ارسال فرمادیں۔ اگر آپ منی آرڈر بھیجنے کی زحمت سے بچنا چاہتے ہیں تو اپنا پتا ہمیں بذریعہ ای میل، ایس ایم ایس یا ہماری ویب سائٹ پر موجود فارم کے ذریعے بھیج دیں اور ہم آپ کو ماہنامہ کمپیوٹنگ کا تازہ ترین دستیاب شمارہ بذریعہ وی پی پی ارسال کردیں گے۔ اس طرح پہلا شمارہ آپ کے حوالے کرتے ہوئے پوسٹ مین آپ سے سالانہ خریداری کی رقم وصول کرلے گا۔ اس کے علاوہ آپ براہ راست ہمارے بینک اکاؤنٹ میں بھی رقم جمع کرواسکتے ہیں۔

منی آرڈر ارسال کرنے کا پتا

"ماہنامہ کمپیوٹنگ"
57 پریس چیمبرز،
آئی آئی چندریگر روڈ، کراچی

وی پی پی اور دیگر معلومات کے لئے
0342-2507857
http://www.computingpk.com

نوٹ: منی آرڈر پر اپنا نام و پتا ضرور تحریر کریں

بینک اکاؤنٹ کی تفصیل

بینک: ایچ بی ایل
برانچ: مسلم ٹاؤن برانچ، کراچی
اکاؤنٹ ٹائٹل: **MONTHLY COMPUTING**
اکاؤنٹ نمبر: **04007901559103**

نوٹ: رقم جمع کرانے کی بینک آپ سے کوئی فیس طلب نہیں کرے گا۔ رقم جمع کروانے کے بعد اپنی معلومات سے ہمیں بذریعہ فون یا ای میل ضرور مطلع فرمائیں

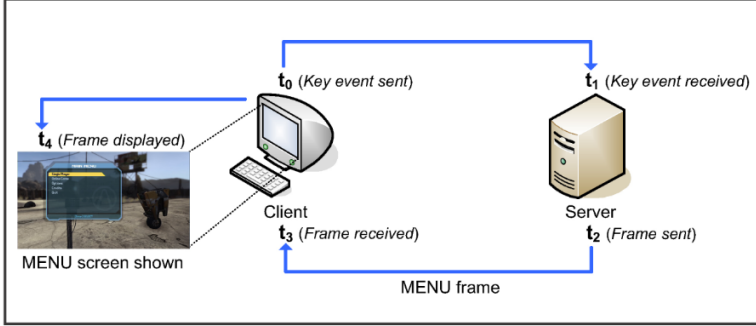
اداریہ

1952ء میں جب پاکستان میں قدرتی گیس جسے ہم سوئی گیس کے نام سے زیادہ جانتے ہیں، دریافت ہوئی، اس نعمت کو ہمارے توانائی کے تمام مسائل کا بہترین حل مان لیا گیا۔ کھاد کی تیاری سے لے کر بجلی بنانے تک اور فیکٹریوں کے بوائلر چلانے سے ہیٹر چلانے تک، سب کام قدرتی گیس کے ذمے لگا دیے گئے۔ پھر 1982ء میں ہائیڈروکاربن ڈیویلپمنٹ انسٹی ٹیوٹ آف پاکستان نے کراچی میں پہلا آزمائشی سی این جی اسٹیشن قائم کیا اور 1989ء میں ایسا ہی ایک اسٹیشن اسلام آباد میں لگایا گیا۔ 1992ء میں حکومتِ پاکستان نے سی این جی کے حوالے سے قوانین تشکیل دیے۔ 1998ء میں حکومت نے ہدف متعین کیا کہ اگلے دو سالوں میں ڈیڑھ سو سی این جی اسٹیشنز قائم کئے جائیں گے اور ایک لاکھ گاڑیوں کو سی این جی پر منتقل کر دیا جائے گا۔ عوام جو پہلے ہی غربت کے "مزے" لے رہی تھی، اس سستے ایندھن کی جانب ایسی دوڑی کہ چند ہی سالوں میں پاکستان سی این جی پر چلنے والی گاڑیوں کی تعداد کے اعتبار سے اوّل نمبر پر آ گیا۔ سرمایہ کاروں نے اربوں روپے کی سرمایہ کاری کر کے ملک کی ہر گلی اور نکڑ پر سی این جی اسٹیشن قائم کر دیے۔ بینکوں نے خوب سستے قرضے بانٹے اور روڈوں پر گاڑیوں کا سیلاب آ گیا۔ ملک میں "اسمبل" ہونے والی گاڑیوں میں بھی پہلے سے ہی سی این جی کِٹ لگائی جانے لگی۔ یوں صرف ایک دہائی میں ملک کے طول و عرض میں ہر چھوٹی بڑی گاڑی سی این جی پر دوڑنے لگی۔ اب اس پالیسی کا نتیجہ کیا نکلا ہے وہ ہم سب کے سامنے ہے۔ ملک میں گاڑیوں میں ڈالنے کے لئے سی این جی ہے نہ گھروں میں چولہے جلانے کے لئے گیس ہے۔ فیکٹریوں کی پیداوار گھٹ گئی ہے، کھاد بیرون ملک سے منگوانی پڑ رہی ہے اور بجلی کا تو ذکر کرنا بھی تکلیف دیتا ہے۔ گیس کی قیمت کو الگ پر لگ گئے ہیں۔ جب پالیسی سازوں کو ہوش آیا اس وقت تک بہت دیر ہو چکی تھی۔ اب سی این جی اسٹیشن چوری چھپے چلتے ہیں، ہوٹل، فیکٹریاں، حتیٰ کہ گھروں میں بھی گیس چوری شروع ہو گئی ہے۔ پہلے پٹرول اور ڈیزل سے جنریٹر چلتے تھے، پھر وہ بھی سوئی گیس پر منتقل ہو گئے۔ یعنی عوام نے قانون شکنی کے لئے نت نئے چور دروازے ڈھونڈ نکالے ہیں۔

اب آیئے ذرا ٹیکنالوجی کی بات کرتے ہیں۔ پاکستان میں یوٹیوب کو بند ہوئے ماہ ستمبر میں پورے دو سال ہو جائیں گے۔ اس دوران درس و تدریس اور معلومات تک رسائی کی اہمیت کا ادراک رکھنے والے ہر شخص نے یوٹیوب کھولنے کے لئے رو پیٹ کر دیکھ لیا، لیکن یوٹیوب نہ کھلی۔ نتیجہ کیا نکلا؟ عوام نے ایک بار پھر چور دروازے ڈھونڈنا شروع کر دیئے۔ پراکسی سرورز، ورچوئل پرائیوٹ نیٹ ورکس اور پرائیوٹ سرورز جن سے پہلے لوگوں کی محدود تعداد واقف تھی، اب ہر کسی کو ان کے بارے میں پتا ہے۔ اگر حالیہ کچھ عرصے میں آپ کو کسی انٹرنیٹ کیفے میں جانے کا اتفاق ہوا ہو تو آپ نے وہاں کمپیوٹرز پر مائیکروسافٹ آفس تو شاید نہ دیکھا ہو، البتہ ہاٹ اسپاٹ شیلڈ ضرور دیکھی ہوگی۔ یوں عملاً پاکستان میں یوٹیوب تو چھوڑیں، ہر بے حیاء ویب سائٹ کو روکنا ناممکن ہو گیا ہے۔ اگر ہاٹ اسپاٹ شیلڈ سے یوٹیوب کھولی جا سکتی ہے، تو کیا بے ہودہ ویب سائٹ کھولنے پر کوئی پابندی ہے؟ اسے پالیسی سازوں کی کم عقلی سمجھیں یا مستقبل بینی کی محدود صلاحیت، لیکن پاکستانیوں کو چور دروازے ڈھونڈنے پر وہ خود مجبور کرتے ہیں!

آپ کا دوست

امانت علی گوہر

مائیکروسافٹ ریسرچ کی اچھوتی کھوج، کلاؤڈ ویڈیو گیمنگ کی ایک بڑی خامی دُور

گزشتہ چند سالوں کے دوران کلاؤڈ کمپیوٹنگ نے زبردست عروج حاصل کیا ہے۔ کلاؤڈ اسٹوریج، کلاؤڈ ویب سائٹ، کلاؤڈ پروسیسنگ سمیت درجنوں دیگر ٹیکنالوجیز کلاؤڈ پر منتقل ہو چکی ہیں۔ لیکن ویڈیو گیمنگ اب تک کلاؤڈ پر اتنی عمدہ کارکردگی نہیں دِکھا سکی جس کی توقع کی جاتی ہے۔ حالانکہ اس سلسلے میں آن لائیو اور این ویڈیا جیسی کمپنیاں سرتوڑ کوششیں کر رہی ہیں۔

جس تیزی سے کم پروسیسنگ پاور والے اسمارٹ فونز اور ٹیبلٹس عام ہو رہے ہیں، ویسے ہی مشکل اور زیادہ پروسیسنگ پاور کے متقاضی کاموں کو کلاؤڈ سرورز پر انجام دینے کا رجحان بڑھ رہا ہے۔ بڑے ویڈیو گیمز کے لئے بھی پروسیسنگ پاور بھی زیادہ درکار ہوتی ہے جو کہ عموماً ایک کم قیمت اسمارٹ فون میں نہیں ہوتی۔ اس لئے ایسی پروسیسنگ کو کلاؤڈ سرور جہاں پروسیسنگ پاور کا کوئی مسئلہ درپیش نہیں، انجام دینا ایک قابل عمل کام لگتا ہے۔ تاہم اس میں نیٹ ورک latency (ڈیٹا کا ایک جگہ سے دوسری جگہ پہنچنے کے لئے درکار وقت) ایک بڑی چٹان کی طرح حائل ہے۔

موجودہ کلاؤڈ گیمنگ پلیٹ فارمز جیسے آن لائیو اور این ویڈیا گرڈ (Grid) میں کوالٹی اور رفتار دونوں بیک وقت ممکن نہیں۔ ان پلیٹ فارمز پر گیم کھیلتے صارف کی دی ہوئی اِن پٹ کو انٹرنیٹ کے ذریعے کلاؤڈ سرور تک پہنچایا جاتا ہے جو اسے پروسیس کر کے گیم میں نئی شبیہ یا فریم (frame) تشکیل دیتا ہے۔ یہ فریم پھر بذریعہ انٹرنیٹ صارف کی اسکرین پر ظاہر ہوتی ہے۔ ظاہر ہے اس میں لوکل ہارڈ ویئر پر پروسیسنگ کے مقابلے میں بہت زیادہ وقت صرف ہوتا ہے۔ صارف کی ڈیوائس سے سرور اور سرور سے ڈیوائس تک واپسی کا سفر round trip time یا RTT کہلاتا ہے۔ راؤنڈ ٹرپ ٹائم کو کم سے کم رکھنے کے لئے کلاؤڈ گیمنگ سسٹم کم ریزولوشن اور انتہائی سخت قسم کی کمپریشن (compression) الگورتھم استعمال کئے جاتے ہیں۔

مائیکروسافٹ ریسرچ کے محققین نے اس مسئلے کا ایک اور حل نکال لیا ہے۔ DeLorean نامی یہ سسٹم صارف کی دی ہوئی گزشتہ اِن پٹ کے مطابق اس کی اگلی حرکت یا اِن پٹ کے بارے میں پیش گوئی کرتا ہے۔ مائیکروسافٹ کے مطابق اس سسٹم کے استعمال سے موجودہ پلیٹ فارم پر ضائع ہونے والے قیمتی 250 ملی سیکنڈ بچائے جا سکتے ہیں۔ جس سے ویڈیو گیمز کو موبائل انٹرنیٹ پر کھیلنا بھی ممکن ہو جاتا ہے۔

ہوتا کچھ یوں ہے کہ DeLorean پر مبنی گیمنگ سرور صارف کی اگلی ممکنہ اِن پٹ کے مطابق پہلے سے ہی فریم تیار کر کے ڈیوائس کے حوالے کر دیتا ہے۔ جیسے ہی صارف اپنی اگلی اِن پٹ دیتا ہے، گیم اس اِن پٹ کے مطابق، پہلے سے موجود فریم ڈیوائس پر ظاہر کر دیتا ہے۔ اس سے وقت کی زبردست بچت ہوتی ہے۔ محققین نے Doom 3 اور Fable 3 ویڈیو گیمز کو DeLorean کے مطابق ڈھالا تو latency میں زبردست کمی واقع ہوئی اور ویڈیو گیم بغیر کسی رکاوٹ کے چلتا رہا۔ ڈی لوریئن کی کامیابی کا دارومدار اس کی کامیاب پیش گوئی پر ہوتا ہے جسے ممکن بنانے کے لئے محققین نے اس میں زیادہ تر صارفین کے گیم کھیلنے اور آگے بڑھنے کے طریقوں کا ڈیٹا شامل کیا۔ ساتھ ہی اسے صارف کی دی ہوئی سابقہ ہدایات یا اِن پٹ سے سیکھنے کے قابل بھی بنایا۔ غلط پیش گوئی کی صورت میں یہ سسٹم غلط فریم کو درست کرنے کی صلاحیت بھی رکھتا ہے۔

AMD کی سالڈ اسٹیٹ ڈرائیوز بھی فروخت کے لئے پیش

گزشتہ چند سالوں میں مائیکروپروسیسر بنانے کے لئے معروف کمپنی AMD نے مائیکروپروسیسرز اور گرافکس کارڈز کے علاوہ دیگر مصنوعات بنانے اور فروخت کرنے کی کوششوں میں اضافہ کیا ہے۔ کمپنی نے سال 2012ء میں SeaMicro نامی کمپنی خرید کر اپنے سرورز تیار کرنا شروع کر دیئے۔ جبکہ سونی پلے اسٹیشن 4 اور ایکس باکس ون کے لئے بھی اے ایم ڈی نے modified چپس ڈیزائن کیں۔ Radeon سیریز کی میموری بھی اے ایم ڈی کی ایک حالیہ پراڈکٹ ہے۔

اب اے ایم ڈی ایک قدم مزید آگے بڑھتے ہوئے سالڈ اسٹیٹ ڈرائیوز (SSD) کے کاروبار میں بھی داخل ہو رہا ہے۔ اس مقصد کے لئے AMD نے OCZ کمپنی سے معاہدہ کیا ہے۔ یہ کمپنی اے ایم ڈی کے لئے اس کی خواہشات کے مطابق سالڈ اسٹیٹ ڈرائیوز تیار کرے گی۔ یاد رہے کہ ریڈیئن برانڈ کی میموری بھی اے ایم ڈی خود تیار نہیں کرتا۔ اس قسم کے معاہدوں سے اے ایم ڈی کو نئی مصنوعات بنانے کے لئے نہ تو نئے پلانٹ لگانے پڑتے ہیں اور نہ ہی نئے آلات خریدنے پڑتے ہیں۔ یوں اے ایم ڈی ابتدائی سرمایہ کاری کی مد میں ایک بڑی رقم خرچ کرنے سے بچ جاتا ہے۔

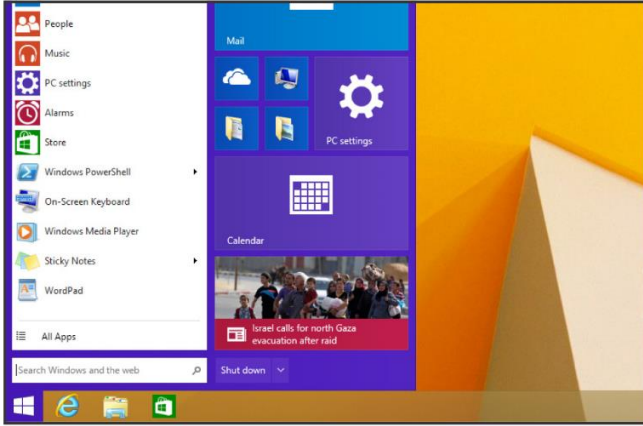
OCZ کمپنی سال 2002ء میں قائم کی گئی تھی اور اس کا مرکزی کاروبار سالڈ اسٹیٹ ہارڈ ڈرائیوز اور پاور سپلائی یونٹس کی تیاری تھا۔ اس کمپنی نے کئی اعلیٰ معیار کی سالڈ اسٹیٹ ہارڈ ڈرائیوز جنہوں نے رفتار کے نئے ریکارڈ بنائے، مارکیٹ میں فروخت کے لئے پیش کیں۔ تاہم بعد میں کمپنی کی ہارڈ ڈرائیوز میں کچھ اہم خرابیاں پائی گئیں جنہوں نے کمپنی کی ساکھ اور مالی حالت کو شدید نقصان پہنچایا۔ گزشتہ سال نومبر میں کمپنی دیوالیہ ہوگئی اور دسمبر میں اسے توشیبا نے خرید لیا۔ تب سے یہ توشیبا کی ایک آزاد کمپنی کی حیثیت سے کام کر رہی ہے۔

AMD نے OCZ کے ساتھ مل کر جس سالڈ اسٹیٹ ڈرائیو سیریز کا اعلان کیا ہے، اس کا نام بھی ریڈیئن (Radeon) رکھا گیا ہے۔ ریڈیئن سالڈ اسٹیٹ ڈرائیوز میں توشیبا کی نئی NAND چپ A19nm استعمال کی گئی ہے۔ ابتداء میں Radeon R7 سیریز میں 120 گیگا بائٹس، 240 گیگا بائٹس اور 480 گیگا بائٹس کی گنجائش والی سالڈ اسٹیٹ ڈرائیوز فروخت کے لئے پیش کی گئی ہیں۔ 120 گیگا بائٹس گنجائش والی سالڈ اسٹیٹ ڈرائیو کی قیمت تقریباً 100 امریکی ڈالر، 240 گیگا بائٹس کی قیمت 164 امریکی ڈالر اور 480 گیگا بائٹس کی گنجائش والی ڈرائیو کی قیمت 290 امریکی ڈالر ہے۔

حالیہ چند سالوں کے دوران سالڈ اسٹیٹ ڈرائیوز کی مانگ میں زبردست اضافہ ہوا ہے۔ عام ہارڈ ڈرائیوز کے مقابلے میں ان کی زیادہ رفتار اور کم توانائی خرچ ہونا انہیں ہر قسم کی ڈیوائسز کے لئے پسندیدہ بناتا ہے۔ لیپ ٹاپس اور نوٹ بکس جن میں بیٹری کا ایک بڑا حصہ ہارڈ ڈرائیوز کھا جاتی ہیں، سالڈ اسٹیٹ ڈرائیوز کا استعمال پہلی پسند ہے۔ اگرچہ ان کی قیمت ماضی کے مقابلے میں خاصی کم ہو چکی ہے تاہم اب بھی یہ عام ڈرائیوز کے مقابلے میں خاصی زیادہ ہے۔

کمپنی کے مطابق ان کی ڈرائیوز دیگر سالڈ اسٹیٹ ڈرائیوز کے مقابلے میں زیادہ پائیدار اور تیز رفتار ہیں۔ اسی لئے کمپنی ان ڈرائیوز کی 4 سال کی وارنٹی دے رہی ہے جبکہ سالڈ اسٹیٹ ڈرائیو بنانے والی دیگر معروف کمپنیاں مثلاً کنگسٹن، کروشل اور سام سنگ اپنی مصنوعات کی تین سال کی وارنٹی دیتی ہیں۔ صرف SanDisk ہی اپنی مصنوعات کی دس سال کی وارنٹی دیتی ہے۔ اے ایم ڈی کے جاری کردہ اعداد و شمار کے مطابق ریڈیئن آر سیون سیریز کی ڈرائیوز 550 میگا بائٹس فی سیکنڈ کی زبردست رفتار پر ڈیٹا پڑھ اور 530 میگا بائٹس فی سیکنڈ کی رفتار پر ڈیٹا لکھ سکتی ہیں۔

اے ایم ڈی کو سالڈ اسٹیٹ ڈرائیوز کی مارکیٹ میں اپنے قدم مضبوطی سے جمانے کے لئے کافی وقت درکار ہوگا۔ اس مارکیٹ میں کنگسٹن، سام سنگ اور سین ڈسک جیسی کمپنیاں پہلے ہی اپنی لوہا منوا چکی ہیں۔ اس لئے یہ توقع کرنا کہ اے ایم ڈی اس میدان میں چھا جائے گا، خام خیال ہی ہے۔ تاہم صارفین کو معیاری سالڈ اسٹیٹ ڈرائیو منتخب کرنے کے لئے ایک مزید آپشن دستیاب ہو گیا ہے۔

ونڈوز 9 کا پری ویو ورژن 30 ستمبر کو متوقع ہے

ذرائع کے مطابق مائیکروسافٹ کا منصوبہ ہے کہ 30 ستمبر کو ونڈوز 9 کا نمائشی ورژن پیش کر دیا جائے۔ یہ تاریخ حتمی نہیں تاہم مائیکروسافٹ میں موجود ذرائع نے پہلے بتایا تھا کہ ونڈوز 9 کا پری ویو ورژن ستمبر کے آخر یا اکتوبر کے شروع میں جاری ہوگا، اس لیے 30 ستمبر کی پیش گوئی خاصی معقول لگتی ہے۔ ابھی وثوق سے نہیں کہا جا سکتا کہ پری ویو ورژن میں ونڈوز 9 کے ایسے کتنے فیچرز شامل ہوں گے جن کا سب کو بے صبری سے انتظار ہے۔ مگر امید ہے کہ اس میں نیا تیار کیا گیا اسٹارٹ مینو اور ڈیسک پر چلتی ہوئی میٹرو ایپلی کیشنز ضروری ہوں گی۔

کچھ دنوں پہلے یہ خبریں لیک ہوئیں کہ مائیکروسافٹ ونڈوز 9 کا پہلا عوامی پری ویو ورژن ستمبر کے آخر میں یا اکتوبر کے شروع میں جاری کرنا چاہتا ہے۔ اب ذرائع انکشاف کر رہے ہیں کہ مائیکروسافٹ 30 ستمبر کو ایک پریس کانفرنس میں پری ویو ورژن جاری کرے گا۔ ٹیک پری ویو ورژن بھی اسی پریس کانفرنس یا اس کے بعد جاری کیا جا سکتا ہے۔ امید کی جا رہی ہے کہ ونڈوز 8 کے پہلے پبلک پری ویو ورژن کی طرح ہر کوئی ونڈوز 9 کے اس پری ویو ورژن کو ڈاؤن لوڈ کر سکے گا، مگر اس بات کی بھی توقع ہے کہ مائیکروسافٹ اسے شاید ٹیک نیٹ یا ایم ایس ڈی این کے ذریعے ڈویلپرز اور پروفیشنل کے لیے ہی جاری کرے۔ ونڈوز 9 کے build نمبر 9788 کے لیک ہونے والے اسکرین شاٹ میں پی سی سیٹنگ اور ڈیسک ٹاپ پر میٹرو ایپس چلتے دکھائی گئیں ہیں۔

ونڈوز 9 کے ٹیکنالوجی پری ویو ورژن میں بہت سے نئے فیچر ضروری شامل ہوں گے مگر تمام فیچرز کی امید رکھنا بیکار ہے۔ ونڈوز 8 کا جب پری ویو ورژن جاری کیا گیا تھا، وہ بظاہر ونڈوز سیون جیسا ہی محسوس ہوتا تھا۔ تاہم ونڈوز 9 کے بارے میں کہا جا رہا ہے کہ یہ ونڈوز 8 سے بہت مختلف ہے، اس لئے ہم امید کر سکتے ہیں کہ ونڈوز 9 کے پری ویو ورژن میں نئے اور پرانے فیچرز کا چربہ دیکھنے کو ملے گا۔ ونڈوز 9 کا ایک اہم فیچر یہ ہے کہ اس میں Cortana کو مربوط کر دیا گیا ہے۔ لیکن پری ویو ورژن میں اس کے شامل ہونے کی امید کم ہے۔

مائیکروسافٹ 30 ستمبر کے پریس ایونٹ میں Windows RT کے متعلق بھی بتایا جا سکتا ہے جسے اب ونڈوز فون کے ساتھ مربوط کیا جا رہا ہے۔ یہ سب ان کوششوں کا حصہ ہے جس میں مائیکروسافٹ اپنے تمام آپریٹنگ سسٹمز کو یکجا کر رہا ہے۔

رسبری پائی کا نیا ورژن 2017ء سے پہلے ممکن نہیں

کریڈٹ کارڈ کے سائز جتنے کمپیوٹر رسبری پائی کو بنانے والی کمپنی رسبری پائی فاؤنڈیشن کا کہنا ہے کہ انہیں رسبری پائی کی خامیوں کا علم ہے اور وہ اس میں درکار ضروری بہتری کرنا چاہتے ہیں۔ رسبری پائی اس وقت دو ماڈلز میں دستیاب ہے۔ ایک ماڈل (Model A) کی قیمت 25 ڈالر جبکہ دوسرے ماڈل (Model B) کی قیمت 35 ڈالر ہے۔ ان دونوں ماڈلز میں فرق میموری، ایتھرنیٹ پورٹ اور یو ایس بی پورٹس کا ہے۔ رسبری پائی کے شائقین کو شکوہ ہے کہ اس کا ہارڈ ویئر موجودہ دور کی ضروریات سے ہم آہنگ نہیں۔ مثلاً دو یو ایس بی پورٹس کی بورڈ اور ماؤس کو ہی جوڑنے کے لئے استعمال ہو جاتی ہیں اور دوسری ڈیوائسز کو رسبری پائی سے جوڑنا مشکل ہو جاتا ہے۔

رسبری پائی فاؤنڈیشن نے گزشتہ ماہ جولائی میں Model B+ کا اعلان کیا ہے جس کی قیمت 35 ڈالر ہی ہوگی تاہم اس میں یو ایس بی پورٹس کی تعداد 4 ہوگی۔ لیکن اس ماڈل کے بارے میں پیش گوئی کی جا رہی ہے کہ یہ سال 2017ء سے پہلے عام عوام کے لئے دستیاب نہیں ہو سکے گا۔ وجہ یہ بتائی جا رہی ہے کہ رسبری پائی فاؤنڈیشن اس سے پہلے رسبری پائی کے لئے دیگر کمپونینٹس مثلاً ٹچ اسکرین بنانے کا ارادہ رکھتی ہے۔

ہیکرز کا سونی پلے اسٹیشن نیٹ ورک پر حملہ اور بم کی جعلی خبر سے جہاز کی ایمرجنسی لینڈنگ

ہیکرز کے ایک گروپ جس نے اپنا نام لیزرڈ اسکواڈ (Lizard Squad) رکھا ہوا ہے، نے ڈسٹری بیوٹڈ ڈینائل آف سروس اٹیک کے ذریعے سونی پلے اسٹیشن نیٹ ورک کی سروس کو عارضی طور پر معطل کر دیا۔ ان ہیکرز کی شرانگیزی یہیں تک محدود نہیں رہی بلکہ انہوں نے ٹوئٹر کے ذریعے امریکی ایئرلائن کو جعلی خبر دی کہ ان کی پرواز 362 جس میں سونی انٹرٹیمنٹ کے صدر جان سمیڈلے (John Smedley) ڈیلاس سے سان ڈی ایگو جا رہے ہیں، میں دھماکہ خیز مواد موجود ہے۔ اس خبر کے ملتے ہی امریکی ایئرلائن نے پرواز کا رُخ موڑ کر اسے فوراً Phoenix ایئرپورٹ پر لینڈ کروا دیا۔

ڈسٹری بیوٹڈ ڈینائل آف سروس سائبر حملے کی ایک قسم ہے جس میں ہیکرز دنیا بھر سے اپنے قابو میں کئے ہوئے کمپیوٹرز کے ذریعے کسی سرور پر کثیر تعداد میں درخواستیں بھیجتے ہیں جن کے جواب دینا سرور کے بس سے باہر ہو جاتا ہے اور وہ سب کے لئے غیر دستیاب ہو جاتا ہے۔ اس قسم کے حملے عام ہیں اور آئے روز مختلف ویب سائٹس اور سرورز اس کا نشانہ بنتے ہیں۔ لیزرڈ اسکواڈ نے سونی پلے اسٹیشن نیٹ ورک پر حملہ 24 اگست کو شروع کیا جس کے بعد شمالی امریکہ میں PS3 اور PS4 استعمال کرنے والے صارفین کی اس نیٹ ورک تک رسائی ممکن نہیں رہی۔ حملے کے وقت ہی لیزرڈ اسکواڈ نے ٹوئٹر پر دعویٰ کیا کہ وہ ایکس باکس لائیو، Blizzard سمیت چند دیگر آن لائن گیمنگ سروسز کے سرورز پر بھی DDoS کر رہے ہیں۔ یہ سروسز حملے کے دوران عارضی طور پر معطل یا سست روی کا شکار رہیں لیکن سونی پلے اسٹیشن نیٹ ورک مکمل طور پر ناقابل رسائی ہو گیا۔ اس بات کی تصدیق سونی نے اپنی بلاگ پوسٹ کے ذریعے بھی کی۔ بعد میں یہ نیٹ ورک مکمل طور پر بحال بھی کر دیا گیا۔

ڈسٹری بیوٹڈ ڈینائل آف سروس حملے کی خبر زیادہ اہم نہیں لیکن کسی ہوائی جہاز کی ایمرجنسی لینڈنگ اور وہ بھی ایک جعلی خبر پر ایک غیر معمولی واقعہ ہے۔ ایئرلائنز اور انٹیلی جنس ایجنسیاں جہازوں میں دھماکہ خیز مواد کی موجودگی کی اطلاعات کو انتہائی سنجیدگی سے لیتی ہیں۔ ماضی میں کئی افراد کو اس قسم کی افواہوں پر گرفتار کیا جا چکا ہے۔ اس کیس میں ایئرلائن کی سنجیدگی کی وجہ خبر میں پرواز کے نمبر اور سونی کے صدر کی موجودگی کی درست اطلاع تھی۔ جس سے ایئرلائن کو محسوس ہوا کہ یہ خبر درست بھی ہو سکتی ہے۔ تاہم لینڈنگ کے بعد جہاز کی تلاشی سے یہ خبر جھوٹ ہی ثابت ہوئی۔ سونی نے اپنے ایک بیان میں اس حوالے سے تبصرہ کیا ہے کہ امریکی ادارہ ایف بی آئی اس سائبر حملے اور جھوٹی افواہ کے پیچھے موجود افراد تک پہنچنے کی کوشش کر رہا ہے۔

یاد رہے کہ اپریل 2011ء میں بھی سونی پلے اسٹیشن نیٹ ورک پر سائبر حملہ کیا گیا تھا جس کے نتیجے میں یہ سروس پورے ایک ماہ تک آف لائن رہی تھی۔

گوگل اب نتائج میں آتھرشپ نہیں دکھائے گا

گوگل نے اعلان کیا ہے کہ اب وہ گوگل پر کئی جانے والے سرچنگ کے نتائج میں آتھرشپ نہیں دکھائے گا۔ اس کا مطلب یہ ہے کہ اب نتائج میں ظاہر ہونے والے مضامین کے ساتھ انہیں تحریر کرنے والے گوگل پلس کے صارفین کی پروفائلز نہیں دکھائی جائیں گی۔ گوگل نے اس سال جون میں نتائج میں ظاہر ہونے والے مضامین کے ساتھ انہیں لکھنے والے مصنّفین کی تصاویر دکھانا بند کر دیا تھا۔ گوگل کے مطابق اس کی توقعات کے برعکس یہ معلومات اس کے صارفین کے لئے کوئی خاص معاون ثابت نہیں ہو رہی۔ تاہم گوگل نے یہ بھی کہا ہے کہ وہ نتائج میں صارف کے گوگل پلس پر موجود دوستوں کی پوسٹس اور متعلقہ پیجز دِکھاتا رہے گا۔

گوگل نے آتھرشپ پروگرام کا آغاز جون 2011ء میں کیا تھا۔ اس کے بعد اس پروگرام کے فیچرز میں کئی اضافے اور تبدیلیاں کی گئی ہیں مگر اب اسے مکمل طور پر ختم کرنے کا فیصلہ کر لیا گیا ہے۔ لہٰذا وہ ویب ماسٹرز جنہوں نے اپنی ویب سائٹس پر مخصوص مارک اپ rel=author شامل کیا تھا، وہ اسے حذف کر سکتے ہیں۔

مائیکروسافٹ ونڈوز کے لئے گوگل کروم کا 64 بٹ بی ٹا ورژن جاری

گوگل نے ایک لمبے انتظار کے بعد آخر کار مائیکروسافٹ ونڈوز کے لئے گوگل کروم کا 64 بٹ بی ٹا ورژن جاری کر دیا ہے۔ اس کا مطلب یہ ہے کہ جلد ہی اس کا فائنل ورژن بھی متوقع ہے۔

انٹرنیٹ ایکسپلورر کو گوگل کروم اور موزیلا فائر فاکس پر اس لحاظ سے برتری حاصل رہی ہے کہ اس کا 64 بٹ ورژن ایک عرصے سے موجود ہے جبکہ یہ دونوں اب تک اپنا 64 بٹ فائنل ورژن جاری نہیں کر سکے ہیں۔

گوگل کے مطابق 64 بٹ بی ٹا ورژن انسٹال کرنے والے صارفین اگر پہلے سے 32 بٹ ورژن استعمال کر رہے ہیں تو اس میں محفوظ تمام پاس ورڈز، بک مارکس اور ڈیٹا نئے ورژن میں امپورٹ کر دیا جائے گا۔

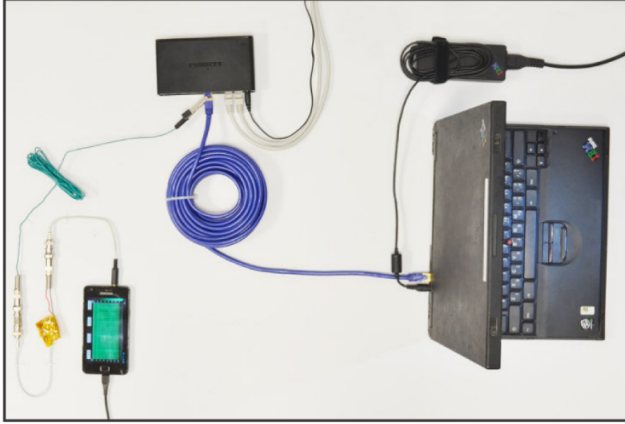
64 بٹ آپریٹنگ سسٹمز ایک دہائی سے موجود ہیں جبکہ 64 بٹ پروسیسرز کو بھی مارکیٹ میں آئے ہوئے اتنا ہی عرصہ ہو چکا ہے۔ انٹل کے گزشتہ پانچ، چھ سالوں کے دوران متعارف ہونے والے تقریباً تمام ہی پروسیسر 64 بٹ تھے۔ یہی وجہ ہے کہ صارفین کے زیر استعمال کمپیوٹرز کی ایک بڑی تعداد 64 بٹ آپریٹنگ سسٹم اور پروسیسر پر مبنی ہے۔ 64 بٹ آپریٹنگ سسٹم اور پروسیسر کی خوبی یہ ہے کہ ان پر چلنے والے سافٹ ویئر 4 گیگا بائٹس سے زیادہ ریم استعمال کر سکتے ہیں۔ 32 بٹ آپریٹنگ سسٹم کے لئے 4 گیگا بائٹس سے زیادہ میموری استعمال کرنا ممکن نہیں ہوتا۔ جبکہ فلوٹنگ پوائنٹ کیلکولیشن کرنے والے سافٹ ویئر (مثلاً گرافکس سافٹ ویئر) کی کارکردگی بھی 64 بٹ کمپیوٹر پر بہترین ہوتی ہے۔ 32 بٹ آپریٹنگ سسٹمز کی میموری استعمال کرنے کی محدود صلاحیت کی وجہ سے فائر فاکس اور گوگل کروم جیسے براؤزرز ریم کا ایک بڑا حصہ ہضم کر جاتے ہیں جس کی وجہ سے صارفین کو سست رفتار براؤزرز برداشت کرنے پڑتے ہیں۔

ماضی میں دیکھا گیا کہ ہے کہ گوگل کی اکثر بی ٹا ورژن والی مصنوعات بھی انتہائی مستحکم ثابت ہوتی ہے۔ اس کی ایک مثال جی میل ہے جو ایک عرصے تک بی ٹا ورژن میں رہا۔ لہٰذا توقع ہے کہ گوگل کروم کا یہ بی ٹا ورژن بھی بہت مستحکم ہوگا۔

اوپرا اور مائیکروسافٹ کا معاہدہ، نوکیا کے کچھ اسمارٹ فونز پر اوپرا ویب براؤزر انسٹال ہوگا

اوپرا اور مائیکروسافٹ نے ایک معاہدے پر دستخط کر دیئے ہیں جس کے تحت نوکیا کے کچھ موبائل فونز میں انٹرنیٹ ایکسپلورر یا کسی دوسرے ویب براؤزر کے بجائے اوپرا انسٹال ہوگا۔ ابتداء میں نوکیا آشا (Asha) سیریز کے موبائل فونز میں اوپرا شامل کیا جائے گا۔ جبکہ معاہدے میں سیریز 30+ اور سیریز 40 کے کم قیمت والے موبائل فونز پر بھی اوپرا کے استعمال کا عندیہ دیا گیا ہے۔ اس معاہدے کا نوکیا لومیا سیریز پر کوئی اثر نہیں پڑے گا جس میں بطور آپریٹنگ سسٹم مائیکروسافٹ ونڈوز فون استعمال ہوتا ہے۔ ونڈوز فون میں انٹرنیٹ ایکسپلورر ہی بطور ویب براؤزر استعمال ہوگا۔

ڈیسک ٹاپ کمپیوٹرز پر اوپرا کا استعمال انتہائی محدود ہوگیا ہے۔ تاہم اسمارٹ فونز پر اب بھی اوپرا (Opera Mini) کا استعمال بڑے پیمانے پر کیا جا رہا ہے اور کا مقابلہ ایپل سفاری اور گوگل کروم سے کیا جا سکتا ہے۔ موجودہ ویب براؤزرز میں دستیاب فیچرز کی ایک بڑی تعداد کا موجد اوپرا ہے۔

کمپیوٹر کو چھو کر کرپٹوگرافک کلید معلوم کی جا سکتی ہے

تل ابیب یونی ورسٹی، اسرائیل میں سکیورٹی ماہرین کی ایک ٹیم نے کمپیوٹر کو چھو کر اس میں محفوظ کرپٹوگرافک کلید (Cryptographic Key) معلوم کرنے کا عملی مظاہرہ پیش کیا ہے۔ کمپیوٹرز کے بارے میں ایک حقیقت یہ ہے کہ جب ان کا مائیکرو پروسیسر حسابی عمل (computation) کر رہا ہوتا ہے، کمپیوٹر کے گراؤنڈ الیکٹریکل پوٹینشل میں اس کمپیوٹیشن کے عمل کے مطابق کمی و بیشی ہوتی رہتی ہے۔ محققین کی مذکورہ ٹیم جس کی سربراہی ایرن ٹرومر (Eren Tromer) کر رہے تھے، اسی حقیقت کا فائدہ اٹھایا۔ ٹرومر کے مطابق لیپ ٹاپ وغیرہ کے دھاتی ڈھانچے یا چیسس کو چھونے سے انسانی جسم میں پیدا ہونے والے الیکٹریکل پوٹینشل یا برقی جھد کی پیمائش اور اس کا سافٹ ویئر الگورتھم کے ذریعے تجزیہ کرنا، کمپیوٹر میں محفوظ خفیہ کلیدوں کو معلوم کرنے کے لئے کافی ہے۔

محققین اپنی تحقیق کے بارے میں مقالہ اگلے ماہ جنوبی کوریا میں ہونے والی ایک کانفرنس میں پیش کریں گے۔ تاہم انہوں نے پہلے ہی سانتا باربرا، کیلی فورنیا میں کرپٹوگرافی کے حوالے سے ہونے والی ایک کانفرنس میں اس کا عملی مظاہرہ پیش کر کے سب کو حیران کر دیا ہے۔ لیپ ٹاپ کے دھاتی ڈھانچے کو چھونے سے جسم میں پیدا ہونے والی الیکٹریکل پوٹینشل کو ایک عام برقی تار جو کلائی یا جسم کے کسی اور حصے سے باندھی گئی ہو، وصول کیا جا سکتا ہے۔ گیلے یا پسینے والے ہاتھ زیادہ بہتر کام کرتے ہیں۔ تاہم چھونے کا عمل ضروری نہیں۔ لیپ ٹاپ کے دھاتی ڈھانچے سے براہ راست بھی تار جوڑ کر اس کے گراؤنڈ الیکٹریکل پوٹینشل کی پیمائش کی جا سکتی ہے۔ نیز، دھاتی ڈھانچہ کے بجائے، یو ایس بی پورٹ، وی جی اے پورٹ یا ایتھرنیٹ کے دھاتی حصے کو بھی استعمال کیا جا سکتا ہے۔ حد تو یہ ہے کہ برقی رو کی پیمائش کرنے والے حساس آلات کے ذریعے لیپ ٹاپ/کمپیوٹر سے کوئی تار یا چھوئے بغیر بھی گراؤنڈ الیکٹریکل پوٹینشل کی پیمائش بھی ممکن ہے۔

ایرن ٹرومر کی ٹیم نے جو سسٹم تیار کیا ہے، اس کے کام کرنے کے لئے صرف ایک شرط ہے کہ جب پروسیسر کرپٹوگرافک ڈیٹا کو کلید یا key کے ذریعے decrypt کر رہا ہو، اسی وقت گراؤنڈ الیکٹریکل پوٹینشل میں ہونے والی تبدیلی کی پیمائش کی جائے۔ ٹرومر کا کہنا ہے کہ انہوں نے اس سسٹم کے ذریعے آج کل زیر استعمال اعلیٰ نوعیت کے کرپٹوگرافک الگورتھم کی کلیدیں (keys) حاصل کرنے میں کامیابی حاصل کی ہے۔ ان کلیدوں میں 4096 بٹ آر ایس اے اور 3072 بٹ الجمل کلیدیں بھی شامل ہیں۔

ایرن ٹرومر اور ان کی ٹیم کی اس تحقیق سے ہارڈ ویئر میں پائی جانے والی خامیوں اور ان کے غلط استعمال کے بارے میں مزید ثبوت مل گئے ہیں۔ کچھ عرصہ پہلے ریسرچرز نے اس بات کا پتا لگایا تھا کہ کسی کمپیوٹر کی بجلی خرچ کرنے کی پیمائش کر کے کرپٹوگرافک کلیدوں کو پتا چلا جا سکتا ہے۔ ساتھ ہی یہ بھی پتا لگایا گیا کہ کمپیوٹر کے بجلی خرچ کرنے کی مقدار کی پیمائش کر کے یہ جانا جا سکتا ہے کہ آیا وہ کسی سائبر حملے کا شکار تو نہیں۔

معروف جریدے ٹیکنالوجی ریویو سے بات کرتے ہوئے اسٹونی بروک یونی ورسٹی کے راڈو سی اون (Radu Sion) کہتے ہیں کہ ایسے درجنوں ہارڈ ویئر سائیڈ چینلز موجود ہو سکتے ہیں جو ابھی دریافت ہونا باقی ہیں اور ہم مستقبل میں ان کے بارے میں سنتے رہیں گے۔ یاد رہے کہ کرپٹوگرافی میں سائیڈ چینل اٹیک، کرپٹوگرافک سسٹمز پر ایسے حملے کو کہا جاتا ہے کہ جس میں الگورتھم کی کمزوریوں کا پتا لگانے یا انہیں توڑنے کے بجائے اس سسٹم کی طبعی تبدیلیوں مثلاً بجلی کے استعمال میں آنے والا فرق، دو مختلف کمپیوٹیشن کے درمیان کے وقت کا فرق وغیرہ کا جائزہ لیا جاتا ہے۔

ایرن ٹرومر بتاتے ہیں کہ ان کے دریافت کردہ سائیڈ چینل حملے سے بچنے کا طریقہ زیادہ مشکل نہیں۔ کرپٹوگرافی سافٹ ویئر بنانے والوں کو کمپیوٹیشن کے دوران اٹکل (random) سے کچھ ڈیٹا بھی شامل کرنا ہوگا۔ GnuPG نامی کرپٹوگرافک سافٹ ویئر بنانے والوں نے پہلے ہی تبدیلیاں کر کے نیا ورژن جاری کر دیا ہے۔

ویئرایبل کمپیوٹرز کے لئے ایک نئی چپ، جو اُن کی بیٹری ٹائمنگ میں اضافہ کردے گی

ویئرایبل (جس کا اردو متبادل پوشیدنی ہے) کمپیوٹرز اب عام ہوتے جارہے ہیں۔ اسمارٹ واچز، اسمارٹ گلاسز اور ان گنت ایسی ڈیوائسز اب فروخت کے لئے دستیاب ہوگئی ہیں، جنہیں پہنا جاسکتا ہے۔ وقت کے ساتھ یہ جدید سے جدید تر ہوتی جارہی ہیں لیکن ان تمام ڈیوائسز کو وہی مسئلہ درپیش رہتا ہے جو کہ عام طور پر ایک اسمارٹ فونز کو ہوتا ہے، یعنی بیٹری ٹائمنگ۔ ویئرایبل کمپیوٹرز یا ڈیوائسز میں چھوٹی بیٹریاں نصب ہوتی ہیں جن کی طاقت بھی محدود ہوتی ہے۔ لہٰذا انہیں دن میں ایک بار ضرور چارج کرنا پڑتا ہے، چاہے آپ ڈیوائس کو کتنا ہی کم استعمال کریں۔ گوگل گلاس اس کی ایک اہم مثال ہے۔ اس مسئلے کا ایک ممکنہ حل 2010ء میں قائم کی گئی کمپنی Ineda Systems نے پیش کیا ہے۔ انہوں نے ایک خاص طرح کی چپ ڈیزائن کی ہے جو کہ ڈیوائس کے مرکزی پروسیسر کے ساتھ ملکر کام کرتی ہے۔ یہ چپ معمولی کام جیسے ڈیوائس پہنے شخص کی آواز پر کان لگائے رکھنے اور سادہ ایپلی کیشنز چلانے کا کام خود انجام دیتی ہے تا کہ مرکزی پروسیسر سوتا رہے اور بیٹری ضائع نہ ہو۔ انیڈا اسسٹمز کے نائب صدر اجیتھ دساری کہتے ہیں کہ ہم نے صارفین کے ویئرایبل کمپیوٹرز کو استعمال کرنے کے طور طریقوں کا مطالعہ کیا اور انہیں کو ذہن میں رکھتے ہوئے یہ چپ ڈیزائن کی۔ ویئرایبل کمپیوٹرز نوے فی صد وقت میں یا تو استعمال نہیں ہورہے ہوتے یا پھر سادہ ایپلی کیشنز چلا رہے ہوتے ہیں۔ اس لئے ڈیوائس کے پروسیسر کو چلاتے رہنے سے ان کی بیٹری غیر ضروری طور پر ضائع ہوتی ہے۔

انیڈا اسسٹمز کے مطابق وہ ابھی دو مختلف چپس کی جانچ پڑتال کررہے ہیں اور ان کا ہدف ہے کہ اگلے سال تک ان چپس کی تجارتی پیمانے پر تیاری شروع کردی جائے۔ ان دو مختلف چپس میں micro نامی چپ میں دو پروسیسر کورز جبکہ advanced چپ میں تین پروسیسرز کورز نصب ہیں۔ ان چپس میں ایک پروسیسر کور جس کی پروسیسنگ قوت کم ہے اور وہ بجلی بھی بہت کم خرچ کرتا ہے، ہمیشہ چلتا رہتا ہے۔ جبکہ دیگر پروسیسر کورز اُس وقت چلائے جاتے ہیں جب زیادہ کمپیوٹنگ پاور درکار ہوتی ہے۔ اگر درکار کمپیوٹنگ پاور فراہم کرنا تمام پروسیسر کورز کے بس کی بات نہ رہے تو ڈیوائس کے مرکزی پروسیسر کو جگایا جاتا ہے۔

انیڈا اسسٹمز کا ایڈوانسڈ چپ جس میں تین پروسیسر کورز ہیں، اعلیٰ نوعیت کی اسمارٹ واچز کے لئے تیار کیا گیا ہے۔ اس چپ کا سب سے کمزور پروسیسر عمومی نوعیت کے کام جیسے موشن سینسر کی مونیٹرنگ، دوسری ڈیوائسز کے ساتھ بلیوٹوتھ کنکشن قائم رکھنا اور ڈیوائس کو جگانے کے لئے دی جانے والی وائس کمانڈ (مثلاً OK, Google) کو پہنچانا بخوبی انجام سے سکتا ہے۔ دوسرا پروسیسر کورگانے بجانے، پیچیدہ وائس کمانڈ کو سمجھنے اور قدرے پیچیدہ ایپلی کیشنز کو چلانے کی صلاحیت رکھتا ہے جبکہ تیسرا پروسیسر کور ان دونوں کے مقابلے میں زیادہ پیچیدہ کام مثلاً speech recognition انجام دے سکتا ہے۔ دساری کہتے ہیں کہ دو پروسیسر کور والی چپ یعنی micro کو کم سہولیات رکھنے والی اسمارٹ واچز، اسمارٹ فونز اور دیگر چھوٹے ییئرایبل کمپیوٹرز میں استعمال کیا جا سکے گا۔

امکان ہے کہ اسمارٹ واچز سے پہلے ہی انیڈا کی تیار کردہ چپس اسمارٹ فونز میں استعمال کی جائیں گی۔ اسمارٹ فونز بنانے والی کچھ کمپنیوں نے پہلے ہی انیڈا اسسٹمز کی چپس جیسی مددگار چپس اپنے اسمارٹ فونز میں شامل کررکھی ہیں۔ مثلاً موٹورولا Moto X میں ایک مائیکرو چپ صرف صارف کے منہ سے OK, Google سننے کے لئے مخصوص ہے۔ جبکہ ایپل آئی فون 5S میں موشن سینسر کے ڈیٹا کو پروسس کرنے کے لئے ایک علیحدہ چپ نصب ہے۔

انیڈا اسسٹمز کی چپس کو اسمارٹ واچز یا اسمارٹ فونز میں استعمال کرنے سے پہلے ان ڈیوائسز پر چلنے والے آپریٹنگ سسٹم اور ایپلی کیشنز میں تبدیلیوں کی ضرورت پیش آئے گی تا کہ وہ اس قسم کی ڈیزائن پر کام کرسکیں۔ اجیتھ دساری اس مسئلے سے واقف ہیں اور کہتے ہیں کہ ان کی کمپنی ایسے سافٹ ویئر ٹولز پر کام کررہے ہیں جو اس مسئلے پر قابو پانے میں معاون ہونگے۔

گوگل کا خودکار طور پر اڑنے والے ڈرونز کے ذریعے ڈیلیوری کا خفیہ پروجیکٹ "وِنگ"

گوگل کو خودکار طور پر چلنے والے گاڑی (self-driving car) پر کام کرتے ہوئے کئی سال ہو گئے ہیں اور یہ گاڑی تیزی سے کامیابی کی منزلیں طے کر رہی ہے۔ اب گوگل نے اپنے ایک اور خفیہ پروجیکٹ "وِنگ" جو ڈرونز کے ذریعے اشیاء کو منزل مقصود تک پہنچانے کا سسٹم ہے، سے پردہ اٹھایا ہے۔ برطانوی نشریاتی ادارے کی خبر کے مطابق گوگل ایکس لیب، جو انوکھے اور خفیہ پروجیکٹس پر کام کرنے کے مشہور ہے، گزشتہ دو سال سے پروجیکٹ ونگ پر کام کر رہی ہے۔

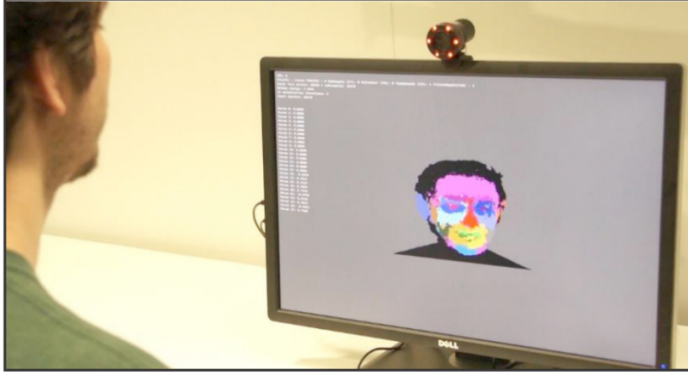
یہ منصوبہ خاصی حد تک ایمزون کے سی ای او جیف بیزوس کے اعلان کردہ ایمزون ڈرونز جیسا ہے جس کا اعلان انہوں نے گزشتہ سال کیا تھا۔ ایمزون ڈرونز کا مقصد ایمزون سے خریدی گئی اشیاء انتہائی کم وقت میں خریدار کے دیئے ہوئے پتے پر بذریعہ ڈرون پہنچانا تھا۔ گوگل کا کہنا ہے کہ اگرچہ اس کے ڈرون اشیاء ایک جگہ سے دوسری جگہ پہنچانے کے لئے استعمال کئے جاسکتے ہیں مگر پروجیکٹ ونگ کا اصل مقصد قدرتی آفات اور تباہی سے متاثرہ علاقوں جہاں زمینی راستوں سے رسائی ممکن نہ ہو، میں ضروری امدادی سامان (مثلاً ادویات) پہنچانا ہے۔ تاہم گوگل ایکس لیب نے اس کے تجارتی استعمال سے بالکل انکار بھی نہیں کیا۔

گوگل نے پروجیکٹ ونگ کی ٹیسٹنگ کے لئے آسٹریلیا کا انتخاب کیا ہے کیونکہ وہ اس حوالے سے قوانین نرم ہیں۔ امریکہ میں اس قسم کے ڈرونز کے لئے پالیسی انتہائی سخت ہے اور ان پر کڑی نظر رکھی جاتی ہے۔ پروجیکٹ ونگ کے ڈرون کی چوڑائی ڈیڑھ میٹر ہے اور اس میں بجلی سے چلنے والے چار پروپلر (Propeller) لگے ہیں۔ ڈرون کا مجموعی وزن تقریباً ساڑھے آٹھ کلو ہے اور یہ ڈیڑھ کلو وزنی سامان اٹھا کر اُڑ سکتا ہے۔ اسے اڑنے اور اترنے کے لئے runway کی ضرورت نہیں اور منزل کے بارے میں ضروری معلومات حاصل کرنے کے بعد یہ خود بخود منزل تک پہنچتا ہے۔ یہ فوجی ڈرون سے مختلف ہے کیونکہ فوجی ڈرونز کو انسان ہی کنٹرول کرتے ہیں۔

کیلی فورنیا میں ایک نیا قانون نافذ، اسمارٹ فون میں kill سوئچ لازمی قرار

امریکی ریاست کیلی فورنیا میں فون چوری اور چھینے جانے کے واقعات میں اضافے کے بعد ایک نیا قانون منظور کیا گیا ہے جس کے تحت یکم جولائی 2015ء کے بعد کیلی فورنیا میں فروخت ہونے والے ہر اسمارٹ فون میں kill سوئچ ہونا لازمی ہوگا۔ اگرچہ یہ قانون ریاست کیلی فورنیا سے باہر اپنے اثر نہیں رکھتا، لیکن ماہرین کہتے ہیں کہ اس قانون کی وجہ سے اسمارٹ فون بنانے والی کمپنیاں kill سوئچ کو جلد ہی اپنے اسمارٹ فونز میں شامل کرنا شروع کردیں گی۔

Kill سوئچ ایک خودکش قسم کی سہولت ہے جو اگر فون میں موجود ہے اور وہ فون چوری ہوجائے تو فون کا اصل مالک اس سہولت کا فائدہ اٹھا کر فون کو بالکل ناکارہ کرسکتا ہے۔ ایپل نے iOS7 میں پہلے ہی ایکٹی ویشن لاک نامی فیچر اس مقصد کے لئے شامل کر رکھا ہے جبکہ چند دیگر موبائل مینوفیکچررز نے بھی اسی قسم کی سہولت فراہم کر رکھی ہے۔

مائیکروسافٹ کے محققین نے عام اسمارٹ فون کیمرے کو تھری ڈی کیمرے میں بدل ڈالا

اسمارٹ فونز کی وجہ سے کیمرا اب ہر جیب میں موجود ہے۔ لیکن گنی چنی جیبی ڈیوائسز ایسی ہیں جن میں کسی شے کی سہ جہتی تصویر کشی یا نقشہ سازی کے لئے depth کیمرے موجود ہیں۔ جیبی ڈیوائسز میں ڈیپتھ کیمروں کی اہمیت میں حالیہ کچھ عرصے کے دوران زبردست اضافہ دیکھا گیا ہے۔ اتنی اہمیت کی وجہ فون جیسی جیبی ڈیوائسز سے ہمارا تعلق ہے۔ ہم اپنے فون سے روڈ، گلی کوچوں سے لیکر اپنے گھر میں اشیاء کی ترتیب تک ہر چیز کی تصویر اتار سکتے ہیں۔ اگر موبائل کیمرے، ڈیپتھ کیمروں کا کام کرنے کے قابل ہوجائیں تو ڈیویلپرز ہمارے اردگرد موجود اشیاء کی سہ جہتی نقشہ سازی کر کے ہمارے کئی کام آسان بنا سکتے ہیں۔ اس کا خاص طور پر فائدہ بینائی سے محروم لوگوں کو ہوگا۔ انہی فوائد کو مدنظر رکھتے ہوئے گوگل نے پروجیکٹ ٹینگو شروع کیا تھا جس کے تحت ڈیپتھ اور تھری ڈی کیمروں سے مزین اسمارٹ فون تیار کیا جانا ہے۔ لیکن دوسری جانب مائیکروسافٹ کے محققین نے ایک عام اسمارٹ فون کیمرے یا ویب کیمرے کو ہی ڈیپتھ کیمرے میں بدلنے کا سستا طریقہ ڈھونڈ نکالا ہے۔

مائیکروسافٹ ریسرچ کے سیئن ریان فنیلو (Sean Ryan Fanello)، کیم کسکن (Cem Keskin) اور شاہرم ازادی (Shahram Izadi) پر مبنی ٹیم نے عام ویب کیمرے میں تبدیلی کرتے ہوئے اس میں سے انفرا ریڈ فلٹر کو ہٹا دیا۔ اس کے بعد انہوں نے ایک نیا فلٹر اس میں شامل کیا جو صرف زیریں سرخ شعاعوں کو ہی گزرنے دیتا تھا۔ اس کے علاوہ کیمرے کے اردگرد چند انفرا ریڈ ایل ای ڈیز بھی لگائی گئیں جو زیریں سرخ شعاعیں خارج کرتی تھیں۔ اس طرح بنیادی طور پر انہوں نے ایک عام کیمرے کو زیریں سرخ شعاعوں والے کیمرے میں بدل دیا۔

محققین کی مذکورہ ٹیم کے مطابق وہ زیریں سرخ شعاعوں کی منعکس ہونے والی شعاعوں کی شدت سے کسی شے کے قریب یا دور ہونے کا اندازہ لگاتے۔ وہ اشیاء جو زیادہ روشن ہیں، وہ قریب ہے جبکہ کم روشن اشیاء دور موجود ہیں۔ ٹیم نے اپنے سسٹم (جو سام سنگ گلیکسی نیکسس اسمارٹ فون اور مائیکروسافٹ لائف کیم ویب کیمرے پر مشتمل تھا) کو اشیاء پہچاننے کی تربیت دی۔ ابتداء میں اس پروجیکٹ کو صرف انسانی ہاتھ اور چہرے کا سہ جہتی نقشہ بنانے تک محدود رکھا گیا ہے۔ تاہم سسٹم کو مزید تربیت دے کر دیگر اشیاء کے سہ جہتی نقشے بنانے کے قابل بھی بنایا جا سکتا ہے۔

صارفین کو للچا کر کلک کرنے پر مجبور کرنے والی پوسٹس کے خلاف فیس بک کا کریک ڈاؤن

ایک تحقیق کے مطابق فیس بک کے ایک تہائی صارفین خبروں کے لئے فیس بک پر انحصار کرتے ہیں۔ یہ وہ خبریں ہوتی ہیں جو صارفین کے لائک کئے ہوئے مختلف پیجز پر شیئر کی جاتی ہیں۔ اس بات کا فائدہ اٹھا کر مختلف ویب سائٹ مالکان تجسس میں مبتلا کر دینی والی تصاویری پوسٹس یا عنوانات شیئر کرتے ہیں تاکہ زیادہ سے زیادہ صارفین ان کی ویب سائٹ پر آئیں۔ اس کا نتیجہ یہ نکلا ہے کہ اب بیکار اور لایعنی قسم کی خبروں کو بھی دلچسپ عنوانات دے کر شیئر کیا جانے لگا ہے۔ اسے click-bait کہا جاتا ہے۔ فیس بک ایسی تمام پوسٹس کو شناخت کرنے کے لئے الگورتھم تشکیل دے دیا ہے اور اب جعلی عنوانات والی پوسٹس صارفین کی نیوز فیڈ میں دکھائی نہیں دیں گی۔

یہ جاننے کے لئے کہ آیا کوئی پوسٹ جعلی تھی کہ نہیں، فیس بک کسی ربط پر کلک کرنے کے بعد آپ کے اس ویب پیج پر گزارے وقت کی پیمائش کرے گا۔ اگر آپ نے کافی وقت اس ویب پیج پر گزارا ہے تو اس کا مطلب ہے کہ وہ مضمون پڑھنے کے قابل ہے۔ بصورت دیگر وہ جعلی عنوان والا کوئی مضمون ہوسکتا ہے۔ یہ خبر فیس بک صارفین کے لئے تو اچھی ہے مگر ہزاروں نیوز ویب سائٹس کے لئے بہت بری ہے۔

لچکدار ڈسپلے اب حقیقت کے مزید قریب پہنچ گئیں

کٹیوا (Kateeva) نامی کمپنی نے اعلان کیا ہے کہ وہ اس سال کے آخر تک لچکدار ڈسپلے تیار کرنے والے آلات مینوفیکچرز کے حوالے کرنا شروع کردے گی۔ یہ قابل اعتماد لچکدار ڈسپلے کی تجارتی پیمانے پر دستیابی کی جانب ایک انتہائی اہم قدم ہے۔

لچکدار ڈسپلے کا تصور ایک عرصے سے موجود ہے اور اس کی کچھ عملی شکلیں بھی موجود ہیں۔ جنوری 2013ء میں سام سنگ نے لاس ویگاس میں منعقدہ کنزیومر الیکٹرانکس شو کے دوران لچکدار ڈسپلے حاضرین کے سامنے پیش کی۔ کمپنی کا کہنا تھا کہ اس سے لچکدار ڈسپلے والے ایسی اسمارٹ گھڑیاں بنائی جاسکتی ہیں جنہیں کلائی پر باندھا جاسکتا ہے یا ایسی ڈیوائسز تیار کی جاسکتی ہیں جنہیں موڑ کر یا تہہ کرکے جیب میں رکھا جاسکتا ہے۔ لیکن یہ پروٹوٹائپ اتنے مستحکم ثابت نہیں ہوئے کہ ان کی تجارتی پیمانے پر تیاری کی جاسکتی۔ کہا جاتا ہے کہ اس لچکدار ڈسپلے کا پروٹوٹائپ پیش کرنے کے بعد سام سنگ میں اس مادے کے حوالے سے تکنیکی مسائل پیدا ہوگئے جو OLED ڈسپلے کو ہوابند کرنے کے لئے استعمال کیا جاتا ہے۔ نامیاتی ایل ای ڈی (OLED) کو آکسیجن اور پانی کے بخارات تباہ کردیتے ہیں۔ حتیٰ کہ پانی یا آکسیجن کے چند مالیکیولز ہی ڈسپلے کو برباد کرنے کے لئے کافی ہیں۔ لہٰذا نامیاتی ایل ای ڈی کا ہوابند ہونا بے ضروری ہوتا ہے۔ سام سنگ نے اپنی لچکدار ڈسپلے کو خم دار ڈسپلے والے موبائل فون کی تیاری میں استعمال کیا ہے۔ لیکن یہ لچکدار ڈسپلے، اپنی جگہ پر جمی ہوئی ہے اور اسے موڑا نہیں جاسکتا۔ یعنی اسے ایک خاص شکل میں موڑ کو پختہ کردیا گیا ہے۔ اس سے ڈسپلے کو ہوابند کرنے میں آسانی ہوئی۔

کٹیوا نے ایک انک جیٹ پرنٹنگ پروسس تیار کرنے میں کامیابی حاصل کرلی ہے جو OLEDs کو ہوابند کرنے کے لئے حفاظتی تہہ لگا سکتا ہے اور یہ پروسس کسی بھی دوسرے پروسس کے مقابلے میں دوگنا تیز رفتار ہے۔ کٹیوا کے مطابق اس کا پروسس کے ذریعے آدھی قیمت میں لچکدار ڈسپلے تیار کی جاسکتی ہیں اور اس پروسس کو ڈسپلے بنانے والے نظام کا حصہ بھی آسانی سے بنایا جاسکتا ہے۔

لچکدار ڈسپلے میں چھوکر استعمال کرنے کی صلاحیت شامل کرنا بھی ایک چیلنج ہے۔ اس وقت جو ٹچ اسکرین بنائی جاتی ہیں ان میں انڈیئم ٹن آکسائیڈ نامی شفاف لیکن بجلی کا موصل مواد استعمال کیا جاتا ہے۔ لچکدار ڈسپلے میں اگر اسے استعمال کیا جائے تو یہ ڈسپلے کو موڑنے پر ٹوٹ پھوٹ جاتا ہے۔ اس مسئلے کو حل کرنے کے لئے ہلسنکی، فن لینڈ کی ایک کمپنی Canatu نے کاربن نینوٹیوبز کا استعمال شروع کیا ہے۔ لچکدار ڈسپلے میں کاربن نینوٹیوبز کا جھال بچھا دیا جاتا ہے۔ چونکہ یہ خود بھی لچکدار ہوتی ہیں، اس لئے لچکدار ڈسپلے کو توڑنے موڑنے پر انہیں کوئی نقصان نہیں پہنچاتا۔ اس کمپنی کی فیکٹری نے گزشتہ سال کام شروع کردیا تھا اور اب تک 30 مختلف کمپنیوں کو پروٹوٹائپ تیار کرنے میں انہوں نے مدد کی ہے۔

گریک راؤپ (Raupp) جو ایری زونا اسٹیٹ یونی ورسٹی میں ڈسپلے ٹیکنالوجی کے ماہر ہیں، کے مطابق سام سنگ اور دیگر فون بنانے والی کمپنیاں اعتدال پسند رویہ اختیار کئے ہوئے ہیں۔ وہ پہلے خم دار ڈسپلے جسے موڑا نہیں جاسکتا، کے ساتھ تجربات کررہے ہیں کہ آیا لچکدار ڈسپلے ان کی توقعات کے مطابق کام کررہی ہے کہ نہیں۔

کہتے ہیں کہ جدید تحقیق نے انسان کو خوف زدہ کر رکھا ہے۔ آج سے کچھ عرصہ پہلے جراثیموں کی دہشت اتنی نہ تھی، اب تو یہ حال ہے کہ مشترکہ صابن استعمال کرنے سے بھی جراثیم پھیلنے کا خطرہ موجود رہتا ہے۔ بات یہیں تک محدود نہ رہی بلکہ اب ہمیں بتایا جاتا ہے کہ دُھلنے کے باوجود نہ صرف برتنوں میں جراثیم رہ سکتے ہیں بلکہ یہ آپ کے کپڑوں میں بھی موجود ہو سکتے ہیں۔ ابھی ہم جراثیموں سے بچ بچاؤ کرنے میں مصروف تھے کہ پتا چلا موبائل فون زیادہ دیر تک کان سے مت لگائیں اور اسے سامنے والی جیب میں بھی مت رکھیں کیونکہ اس کے سگنلز آپ کی صحت کے لیے نقصان دہ ثابت ہو سکتے ہیں۔ اس فہرست کو مزید آگے بڑھائیں تو وائی فائی کی ریڈیائی لہریں آپ کے جسم سے آر پار ہونے کے لیے تیار بیٹھی ہیں۔ ہم جہاں کہیں جائیں سب سے پہلے وائی فائی کا پاس ورڈ مانگتے ہیں لیکن کیا آپ نے کبھی سوچا کہ وائی فائی کی یہ لہریں جو ہر وقت ہمارے اردگرد پھیلی ہوئی ہیں، ہماری صحت کے لیے نقصان دہ ثابت ہو سکتی ہیں؟ آیئے اس حوالے سے ایک غیر جانبدارانہ تجزیہ کرتے ہیں۔

ریڈیائی لہریں ہمیشہ سے مطالعے کا موضوع رہی ہیں کیوں کہ یہ کئی طریقوں سے مدد کرتی ہیں مثلاً ذرائع ابلاغ، جی پی ایس وغیرہ۔ یہی ریڈیو لہریں آپ کو کمپیوٹر ٹیکنالوجی میں لاسلکی کام کرنے کے قابل بناتی ہیں۔ وائی فائی لہریں ریڈیو لہروں پر مشتمل ہوتی ہیں۔ آج وائی فائی اتنا عام ہے کہ آپ وائی فائی کی لہروں میں رات دن گھرے رہتے ہیں۔ کیا آپ کو وائی فائی کی لہروں کی وجہ سے طبّی اثرات کا کوئی تجربہ ہوا ہے؟ آیئے ہم دیکھتے ہیں کہ کیا وائی فائی واقعی خطرناک ہے اور اس کے سگنلز کے صحت پر کیا اثرات مرتّب ہو سکتے ہیں۔

پہلے ہم یہ جائزہ لیں گے کہ وائی فائی کیسے کام کرتا ہے۔ آپ جانتے ہیں کہ وائی فائی روٹر سے شروع ہوتا ہے اور آپ کی وائی فائی ڈیوائسز پر آ کر ختم ہوتا ہے۔ یہ بالکل بلیوٹوتھ اور سیل فون کی طرح کا عمل ہے۔ (دراصل بلیوٹوتھ ٹیکنالوجی وائی فائی ٹیکنالوجی کا ہی ایک حصّہ ہے)۔ اگرچہ سیل فون یا بلیوٹوتھ کے برعکس وائی فائی سگنلز جسم کے کسی خاص حصّے پر مرتکز نہیں ہوتے۔ آپ سیل فون کو دائیں یا بائیں کان سے لگاتے ہیں اور جتنا آپ بات کرتے ہیں اتنا ہی دماغ کے خاص حصّے میں ریڈیو لہریں اتارتے جاتے ہیں اور یہ عمل ہر کال پر دُہرایا جاتا ہے۔ آپ کی کھوپڑی سیل فون کے سگنلز دماغ میں اترنے سے نہیں روک سکتی۔

وائی فائی کی لہریں زیادہ توانائی والی ہوتی ہیں۔ لیکن چوں کہ اس میں ڈیوائسز کو چھونے کے لیے جسم کا کوئی خاص حصّہ مقرر نہیں ہوتا لہٰذا خطرہ مقابلتاً کم تر ہوتا ہے۔ مزید یہ کہ آپ کے جسم اور ڈیوائس میں کچھ فاصلہ ہوتا ہے اس لیے یہ خطرہ مزید کم تر ہو جاتا ہے۔ وائی فائی روٹر میز پر یا دیوار پر لگایا جاتا ہے اور آپ کا روٹر کے پاس دیر تک کھڑے رہنے کا کام نہیں ہو سکتا اس لیے وائی فائی ڈیوائسز استعمال کرتے وقت روٹر آپ کے جسم سے کافی دور ہوتا ہے اور وائی فائی ڈیوائس میں بھی جسم سے فاصلہ ہوتا ہے۔

سیل فون کے معاملے میں آپ اپنا فون بستر پر لے جاتے ہیں اور غالباً سر کے نزدیک رات بھر رکھتے ہیں۔ یہ رات بھر آپ کے سرہانے رہتا ہے اور (زیادہ تر سیلولر سگنلز کی وجہ سے) صحت کے مسائل پیدا کر سکتا ہے۔ دیگر ڈیوائسز جیسے لیپ ٹاپ اور ٹیبلیٹ وغیرہ کی جگہیں بدلتی رہتی ہیں اور آپ انہیں محدود وقت میں استعمال کر کے دور رکھ دیتے ہیں۔ لہٰذا آپ کے جسم کے کسی بھی حصّے پر وائی فائی ریڈیو لہریں مرتکز نہیں ہو پاتیں۔ وائی فائی کا اس طرح سے استعمال سیل فون کے مقابلے میں صحت کے نقصانات کو کم کر دیتا ہے۔

یہاں یہ نہیں کہا جا رہا کہ وائی فائی محفوظ ہے اور یہ نقصان دہ لہریں استعمال نہیں کرتا، تاہم یہ سیل فون کے طریقۂ استعمال سے زیادہ محفوظ ہے۔ اگرچہ سیل

فون کی ریڈیائی لہروں کی توانائی، وائی فائی میں استعمال ہونے والی ریڈیائی لہروں کی توانائی سے کم ہوتی ہے تاہم سیل فون میں ریڈیائی برقی مقناطیسی لہریں جسم کے ایک ہی حصّے پر بار بار اثر انداز ہوتی ہیں۔سائنس دان وائی فائی ٹیکنالوجی میں استعمال ہونے والی ریڈیائی برق مقناطیسی لہروں پر عرصے سے تحقیقات کرتے آرہے ہیں اور انہیں خدشات ہیں کہ وائی فائی لہریں کینسر کا باعث ہوسکتی ہیں تاہم ورلڈ ہیلتھ آرگنائزیشن کی رپورٹ کے مطابق کوئی تحقیق اس ضمن میں فی الحال کسی حتمی نتیجے پر نہیں پہنچ سکی ہے۔اسی رپورٹ میں یہ بھی درج ہے کہ 2011 میں انٹرنیشنل ایجنسی فار ریسرچ آن کینسر (IARC) نے وائی فائی کو ''انسانوں کے لیے ممکنہ کینسر پیدا کرنے والا عاملِ سرطان زا یعنی Carcinogen کا درجہ دیا ہے۔''

وائی فائی کے حوالے سے کچھ ایسے خاص عوامل ہیں جو اسے نقصان دہ بناتے ہیں اور ان عوامل کی معلومات سے ہم ان نقصانات میں بہت حد تک کمی لا سکتے ہیں اور مستقبل میں ان سے متعلق خدشات کا ازالہ کرسکتے ہیں۔

ریڈیائی تعدادِ امواج کے احاطے سے باہر نکلنا آسان بھی نہیں جیسا کہ پہلے ذکر کیا گیا ہے کہ وائی فائی سگنلز ہر جگہ موجود ہیں اور ان کی تعداد میں روز بروز اضافہ ہوتا جارہا ہے۔اگر آپ رات میں اپنا وائی فائی بند کردیتے ہیں تو پڑوس سے آنے والے وائی فائی سگنلز تب بھی آپ کا جسم وصول کررہا ہوتا ہے۔اس کا اندازہ آپ اس بات سے لگا سکتے ہیں کہ جب آپ اپنا وائی فائی رابطہ (کنکٹی ویٹی) کھولتے ہیں تو ڈیوائس آپ کو متعدد وائی فائی رابطے ظاہر کرتی ہے۔جتنے زیادہ نیٹ ورک ہوں گے اتنا ہی زیادہ آپ ریڈیائی لہروں میں شرابور رہیں گے نتیجتاً آپ کی صحت کو اتنا ہی زیادہ خطرات لاحق ہوں گے۔

وائی فائی کیا ہے؟

وائی فائی ایک رجسٹرڈ تجارتی نشان (ٹریڈ مارک) ہے جو وائی فائی الائنس کی ملکیت ہے۔وائی فائی الائنس کے مطابق وائی فائی کوئی بھی وائرلیس لوکل ایریا نیٹ ورک (WLAN) ہے۔اس تعریف کے مطابق وائی فائی میں ربط کے لیے کوئی تار استعمال نہیں کیا جاتا یہ ریڈیائی لہروں کی ٹیکنالوجی استعمال کرتی ہے۔ویبو پیڈیا (webopedia.com) ریڈیو تعدادِ امواج کی تعریف یوں کرتی ہے ''وہ تعدادِ امواج جو برق مقناطیسی طیف (اسپیکٹرم) ریڈیو لہروں کے حصّے میں موجود ہو۔'' یہاں ان مختلف تعدادِ امواج کا تجزیہ پیش کیا جارہا ہے جو ریڈیو برق مقناطیسی شعاعوں کے طیف کے اس حصّے سے تعلق رکھتی ہے جو ذرائع ابلاغ اور مواصلات میں استعمال ہوتی ہیں۔ایف ایم ریڈیو (VHF) یعنی ویری ہائی فریکوئنسی میں کام کرتی ہیں جس کی پہنچ 88 سے 110MHz ہوتی ہے۔اینا لاگ ٹی وی 400-600 MHz، ڈیجیٹل ٹی وی 600-1000MHz، سیل فون 850-1900MHz (0.8-1.9GHz) جو (UHF) یعنی الٹرا ہائی فریکوئنسی کی پہنچ ہے۔جس میں اب 3G اور 4G ٹیکنالوجی میں استعمال ہونے والی تعددِ امواج 2400MHz یعنی 2.4GHz تک آپہنچی ہے۔واضح رہے جتنی زیادہ تعددِ امواج ہوگی اتنی ہی زیادہ توانائی ہوگی چناں چہ اتنی ہی زیادہ صحت کے لیے نقصان دہ ہوگی۔

وائی فائی کے کیریئر سگنل کی پہنچ 2.5GHz ہے جو تقریباً (SHF) یعنی سپر ہائی فریکوئنسی میں ہے۔جن میں کچھ مزید ڈیوائسز 5-6GHz کی پہنچ میں کام کرتی ہیں۔ڈیجیٹل پلس سگنل والی وائی فائی ڈیوائسز سے نکلنے والی لہریں دیواروں، چھتوں، زمینوں اور انسانوں کے اندر سرائیت کر جاتی ہیں۔وائی فائی شعاعوں کو مائیکرو ویو شعاعیں بھی کہا جاتا ہے کیوں کہ مائیکرو ویو شعاعیں 300MHz سے لے کر 300GHz کی پہنچ میں ہوتی ہیں۔

وائی فائی اور انسانی صحت کو لاحق خطرات

1997 میں پہلی بار وائی فائی متعارف کرایا گیا تھا۔تب سے لے کر آج تک محققین اس موضوع پر بے شمار تحقیقات کر چکے ہیں۔ان تحقیقات کے نتائج اگرچہ وائی فائی کے مضر اثرات کی مکمل تصدیق نہیں کرتے تاہم کئی تحقیقات سے جنم لینے والے شکوک دلیل دیتے نظر آتے ہیں۔یہی وجہ ہے کہ عالمی صحت کی تنظیمیں اور صحت کے تحقیقاتی ادارے اور حکومتیں وائی فائی کے حوالے سے انتباہ جاری کرتی نظر آتی ہیں کہ وائی فائی کی لہریں عموماً صحت اور دماغی صحت اور خصوصاً بچوں پر منفی اثر انداز ہوتی ہیں۔یہاں تفصیل سے وائی فائی پر ہونے والی تحقیقات کے نتیجے میں اس کے مضرِ صحت ہونے کا جائزہ لیا جارہا ہے۔

(1) بے خوابی یا نیند میں خلل

آپ نے نوٹ کیا ہے کہ کبھی آپ نے دیر تک وائی فائی استعمال کیا ہو اور خود کو زیادہ دیر تک جاگتا محسوس کیا ہو یا سونے میں بے چینی پائی ہو۔ایسی شکایات عام ہوتی جارہی ہیں۔ان شکایات کے نتیجے میں 2007 میں ایک تحقیق کی گئی جس میں سیل فون استعمال کرنے کے نتیجے میں نیند پر اثرات سامنے آئے (واضح رہے سیل فون کی لہریں وائی فائی لہروں سے کم توانا ہوتی ہیں) اس تحقیق میں حصّہ لینے والوں کو اصل فون سے برق مقناطیسی سگنلز کا سامنا کرایا گیا یا جعلی فون سے

کوئی سگنلز نہیں دیئے گئے۔ وہ افراد جنہوں نے برق مقناطیسی لہروں کا سامنا کیا تھا انھیں سونے میں زیادہ مشکلات پیش آئیں اور دماغی لہروں کی ترتیب میں تبدیلی بھی مشاہدے میں آئی۔ اس سے یہ خیال کیا گیا کہ فون کے قریب سونا، گھر میں دیر تک وائی فائی کے قریب رہنا یا سونا یا ایک ایسی رہائشی عمارت جہاں کئی وائی فائی سگنلز موجود ہوں شدید نیند کی مشکلات پیدا کرسکتا ہے۔ کیوں کہ وائی فائی کی آلودگی کی مسلسل آتی لہریں نیند یا نیند کے اوقات کار میں مداخلت کرتی ہیں کئی لوگوں کے لیے نیند سے محرومی کا عمل زیادہ بڑی مصیبت کی شروعات ہوتی ہے جن میں اعصابی دباؤ اور بے قاعدہ فشارِ خون وغیرہ کا تعلق ناکافی نیند سے بھی ہوتا ہے۔

(2) بچوں کے اذہان اور نشوونما کو نقصانات

بچے خصوصاً وائی فائی کی لہروں سے زیادہ متاثر ہوتے ہیں کیوں کہ ان کا اعصابی نظام بڑھنے اور پروان چڑھنے کے مرحلے میں ہوتا ہے نیز ان کی کھوپڑی زیادہ پتلی اور چھوٹی ہوتی ہے۔ لہٰذا شعاعیں ان کے دماغ کے زیادہ اندر سرائیت کرجاتی ہیں۔ اسی طرح وائی فائی اور سیل فون سے آتی لہریں طبعی خلوی نشوونما میں خلل ڈال سکتی ہیں۔ 2004 میں جانوروں پر کی گئی ایک تحقیق سے پتا چلا کہ وائی فائی کے سگنلز ان کے گردے کی بالیدگی میں تاخیر کا سبب بنے۔ 2009 میں آسٹریا میں کی گئی تحقیق سے اس معلومات کو مزید تقویت ملی۔ لحمیات (پروٹین) کی تالیف میں خلل اتنا شدید ہوتا ہے کہ مصنّفین نے خصوصی طور پر تحریر کیا کہ ''یہ خلیے کی خصوصیت خاص طور پر بافتوں کی پیدائش اور افزائش پر زیادہ اثر ڈالتی ہے، یعنی بچوں اور نوجوانوں میں۔ نتیجے کے طور پر آبادی کا یہ حصّہ بیان کیے گئے اثرات کے لیے اوسط سے زیادہ اثر پزیر ہوگا۔'' مختصراً یہ کہ بڑھتے ہوئے بچوں کی وائی فائی کے ماحول میں پرورش ان کی نشوونما کے خطرات بڑھا دے گی۔ بچوں میں وائی فائی کے دیگر منفی اثرات میں کسی بھی کام خصوصاً مطالعے میں ارتکاز کا فقدان، قلیل المدّت یادداشت پر اثر ہونا، سردرد، تھکاوٹ، نیند میں بے ضابطگی، انہضام کا مسئلہ، بے چینی و پژمردگی وغیرہ شامل ہیں۔

(3) خلیوں کی افزائش پر اثر

ڈنمارک میں نویں جماعت کے کچھ بچوں کو اپنے سر کے نزدیک سیل فون رکھ کر سونے کے بعد مطالعے و دیگر کاموں میں ارتکاز میں مشکلات پیش آئیں تو انھوں نے ایک سبزی پر وائی فائی سے نکلنے والی ریڈیائی لہروں کے اثرات جانچنے کا ایک تجربہ کیا۔ انھوں نے پودے کے ایک مجموعے کو وائی فائی کے ماحول میں رکھا جب کہ دوسرے مجموعے کو وائی فائی سے پاک ماحول میں رکھا۔ وائی فائی کے روٹرز اتنی ہی مقدار میں شعاعیں خارج کررہے تھے جتنا ایک سیل فون کرتا ہے۔ پودے جو وائی فائی کے زیادہ نزدیک تھے وہ نشوونما ہی نہیں پاسکے۔

(4) دماغی کارکردگی کو نقصان

جیسا کہ ڈنمارک کے ہائی اسکول کے بچوں نے ارتکاز میں مشکلات محسوس کیں۔ سائنس دانوں نے دماغی کارکردگی پر 4G ٹیکنالوجی میں استعمال ہونے والی شعاعوں کے اثرات کو دیکھنا شروع کردیا ہے۔ ایم آر آئی ٹیکنالوجی کے ذریعے دماغ پر ایک تحقیق جو گزشتہ برس کی گئی اس میں دیکھا گیا کہ وہ افراد جن کا فور جی شعاعوں سے سامنا ہوا ان کے دماغ کے کئی حصّوں کی سرگرمی میں کمی پائی گئی۔

ایک اور تحقیق جس میں تیس صحت مند رضا کاروں پندرہ خواتین اور پندرہ حضرات پر مشتمل ایک گروپ کا سادہ سا ذہنی یادداشت کا ٹیسٹ لیا گیا۔ پہلے وائی فائی کی شعاعوں کا سامنا کرائے بغیر ان کا ٹیسٹ لیا گیا جس میں عمومی نتائج ظاہر ہوئے۔ اس کے بعد انھیں وائرلیس کی دستیاب جگہ سے پینتالیس منٹ کے لیے 2.4GHz وائی فائی لہروں سے سامنا کرایا گیا۔ ٹیسٹ کے اس حصّے کے دوران ذہنی سرگرمیوں کی پیمائش کی گئی اور خواتین کی ذہنی سرگرمیوں اور توانائی کی سطح میں واضح تبدیلی نوٹ کی گئی۔ تاہم مردوں کا ٹیسٹ بھی زیادہ تسلی بخش نہ رہا۔

(5) پیدائشی نظام پر منفی اثرات

انسانوں اور جانوروں دونوں کے ٹیسٹ سے محققین نے دریافت کیا ہے کہ وائی فائی لہریں مادہ تولید اور ڈی این اے پر منفی اثر ڈالتی ہیں۔

نیز جانوروں پر ایک تحقیق سے یہ پتا چلا ہے کہ کچھ لاسلکی تعددِ امواج بیضہ کی تنصیب کو روک سکتی ہے۔ مطالعے کے دوران چوہوں کو پینتالیس دن تک روزانہ ایک گھنٹے وائی فائی کا سامنا کرایا گیا جس سے ان کے تکسیدی دباؤ (Oxidative Stress) میں نمایاں اضافہ دیکھا گیا۔ وائی فائی کا سامنا کرنے کے نتیجے میں خلیوں کی ٹوٹ پھوٹ اور ڈی این اے کی ساخت پر اثر بھی دیکھا گیا۔

(6) قلب کے دباؤ میں شدت

تھری جی، فور جی یا ایل ٹی ای سیل فون یا وائرلیس کے احاطے میں رہتے

ہوئے اگر آپ اپنا دل تیزی سے دھڑکتا محسوس کرتے ہیں تو یہ آپ کے دماغی ہیجان کا سبب نہیں ہوسکتا ہے۔ 69 قلبی امراض کے مریضوں پر مشتمل ایک مطالعے سے ظاہر ہوتا ہے کہ ان میں سے کئی مریضوں کو برق مقناطیسی تعددِ امواج کا سامنا رہتا ہے۔ جس کا طبعی نتیجہ دل کی دھڑکن کی رفتار میں اضافہ ہے بالکل اسی طرح جس طرح اعصابی دباؤ میں مبتلا شخص کے دل دھڑکنے کی رفتار تیز ہوجاتی ہے۔

(7) کینسر پیدا کرنے کا سبب

اس موضوع پر بہت زیادہ تنازعہ پایا جاتا ہے مگر ایسے کئی مشاہدات سامنے آچکے ہیں جن میں جانوروں کے نمونے ظاہر کرچکے ہیں کہ برق مقناطیسی شعاعوں سے سامنا رسولی بننے کے خطرے میں اضافہ کرتا ہے۔ اگرچہ اس حوالے سے جتنی زیادہ رپورٹیں عام ہیں اتنا ہی زیادہ انسانی مطالعہ محدود ہے۔

(8) برق مقناطیسی زودِ حسّاسیت

(Electromagnetic Hypersensitivity)

ہم انسان صرف گوشت پوست کے انسان نہیں ہم ایک نہایت پیچیدہ برق مقناطیسی نظام بھی ہیں۔ جس کا مطلب یہ بھی ہے کہ ہم بیرونی برق مقناطیسی لہروں سے تعامل کرتے ہیں۔ تاہم گھر کی اور آفس کی ہر برقی ڈیوائسز کو بند کرنے کی کوشش میں ہمیں پتا چلتا ہے کہ ہم ان ڈیوائسز کے کتنے محتاج ہوگئے ہیں۔ مسئلہ یہ ہے کہ ان برق مقناطیسی شعاعوں کا انسانی صحت پر کتنا نقصان دہ اثر پڑتا ہے اسے بہت کم اہمیت دی جاتی ہے۔

برق مقناطیسی تعددِ امواج موبائل فون، مائیکروویو اور دیگر لاسلکی پروٹوکول جیسے بلیوٹوتھ، وائی فائی اور وائی میکس سے نکلی لہروں میں ہم نہائے رہتے ہیں۔ سیل فون بیس اسٹیشن کے نزدیک ہونے سے بھی برق مقناطیسی زودِ حسّاسیت نقصان دے سکتی ہے اور ہماری لاعلمی کے باوجود شہروں میں ایسا ہونا بہت ممکن ہوتا ہے۔

برق مقناطیسی زودِ حسّاسیت ان افراد کو لاحق ہوتی ہے جنھیں کم دورانیے یا کم تعداد میں شعاعوں کا سامنا کرنے سے بھی مختلف عارضے لاحق ہوجاتے ہیں۔ برق مقناطیسی زودِ حسّاسیت کے کچھ اثرات مندرجہ ذیل ہیں۔

☆ چہرے پر گرم اور جلتی ہوئی سنسنی، کسی حد تک دھوپ کی تپش جیسے اثرات ہونا۔

☆ چہرے پر یا جسم کے دیگر حصوں پر سنسناتا یا چبھتا ہوا احساس۔

☆ رطوبت کی جھلّی کا (جیسے حلق اور آنکھوں کے پیچھے) بے حد خشک ہوجانا۔

☆ رطوبت کی جھلّی (جیسے ناک، گلا، کان اور سانس کی نالی) پر بغیر کسی انفیکشن کے ورم آجانا۔

☆ کسی کام میں ارتکاز کا مسئلہ، یادداشت کا کھونا اور چکر آنا۔

☆ سر درد اور متلی ہونا۔

☆ دانتوں اور جبڑوں میں درد۔

☆ پٹھوں اور جوڑوں میں درد۔

☆ قلب کا کانپنا اور زور زور سے دھڑکنا۔

واضح رہے یہ برق مقناطیسی اثرات ہر عام انسان پر ہوسکتے ہیں۔ تاہم زودِ حسّاسیت کے شکار افراد زیادہ خطرے میں ہوتے ہیں۔

افسوس ناک بات یہ ہے کہ برق مقناطیسی زودِ حسّاسیت سے بچنے کا فی الحال کوئی مکمل علاج نہیں۔ سوائے یہ کہ آپ ان لاسلکی لہروں سے جتنا زیادہ بچیں اتنا بہتر ہے۔ تاہم اس سے بھی زیادہ افسوس ناک بات یہ ہے کہ آپ ان لہروں سے بچ نہیں سکتے یہ خصوصاً شہروں میں ہر جگہ موجود ہیں۔

وائی فائی کے حوالے سے دنیا بھر میں کی جانے والی کوششیں

دنیا بھر میں بیشتر اقوام شعاعوں کا سامنا کرنے کا پابند بنانے کے لیے حفاظتی معیارات مقرر کرچکی ہیں ان معیارات کی بنیاد کم دورانیے میں جسم کی بافتوں کے جلنے یا گرم ہونے پر مقرر ہے۔

آخری بار ان رہنما ضوابط کا 90 کی دہائی کے آخر میں (یعنی وائی فائی کے عام ہونے سے قبل) جائزہ لیا گیا تھا۔ لہٰذا یہ معیارات موجودہ دور میں ناکافی ہیں کیوں کہ یہ صحت کے ان غیر حرارتی اثرات کو بیان نہیں کرتے جن کے متعلق آج دنیا بھر کے بے شمار سائنس دان متفکر ہیں۔ متعدد صحت اور ماحولیات کی عالمی، حکومتی اور غیر حکومتی تنظیموں کی جانب سے حفاظتی معیارات کا جائزہ لینے کی ضرورت پر اصرار کے باوجود اس وقت وائرلیس ٹیکنالوجی کے تیار کنندگان اور سہولت فراہم کنندگان کو صرف حکومتی معیارات پورے کرنے کی ضرورت ہوتی (جو نا کافی ہیں جیسا کہ اوپر بیان کیا جاچکا ہے)۔

اس حوالے سے غالباً سب سے مشہور سن 2000 میں شائع ہونے والی اسٹیورٹ رپورٹ ہے جو یوکے (UK) کی حکومت کی جانب سے قائم کردہ ایک کمیٹی نے مائیکروویو شعاعوں کے اثرات جاننے کے لیے شائع کی تھی۔ کمیٹی کے

سربراہ سر ولیم اسٹیورٹ (یو کے حکومت کے سابق اعلیٰ سائنسی مشیر اور ہیلتھ پروٹیکشن ایجنسی کے سربراہ) تھے۔ اسٹیورٹ رپورٹ میں درج تھا کہ حکومت کے قائم کردہ حفاظتی معیار سے کم کی بھی شعاعوں کا سامنا کرنے سے حیاتیاتی اثرات ہوسکتے ہیں۔ اور یہ کہ ان ٹیکنالوجی کے لیے تنبیہی طریقہ اپنانے کی ضرورت ہے۔ 2007 میں اعلیٰ سطح کے سائنس دان، محققین اور صحتِ عامہ کی پالیسی کے ماہرین کے ایک گروپ نے Bioinitiative کے نام سے ایک رپورٹ شائع کی جس میں دو ہزار سے زائد تحقیقات کا جائزہ لیا گیا تھا۔ ان کی حتمی رپورٹ نے موجودہ مقررہ معیار کی حد سے متعلق شدید تحفظات کو اُبھارا اور وائرلیس ٹیکنالوجی کا سامنا کرنے سے برین ٹیومر اور دیگر صحت کے خطرات کے امکانات کو درج کیا۔

اس رپورٹ کے بعد یورپ کی اعلیٰ ماحولیاتی تنظیموں اور ایجنسیوں نے وائی فائی موبائل فون اور ان کے کھمبوں وغیرہ کی شعاعوں کے سامنا کرنے کے معیارات کی حد میں مزید کمی کے لیے فوری اقدامات کرنے کا مطالبہ کیا۔ انھوں نے مشورہ دیا کہ اس میں تاخیر ازبسٹس (صحت کے لیے نقصان دہ ایک ریشے دار کانی Asbestos)، سگریٹ نوشی اور پٹرول میں سیسے کے ذریعے پیدا ہونے والے صحت کے بحران کی طرح نقصان کو جنم دی سکتی ہے۔

جرمن حکومت اپنے شہریوں کے لیے انتباہ جاری کرچکی ہے کہ وہ گھر پر یا کام کی جگہ پر وائی فائی کے استعمال سے اجتناب کریں اور اس کے بجائے کیبل کنکشن استعمال کریں۔

انگلینڈ اور فرانس کے کئی اسکولوں نے اساتذہ اور والدین کی شکایات پر وائی فائی سسٹم نکال دیے۔ 2007 کے آخر میں پیرس میں فرانسیسی کتب خانوں نے عملے کی جانب سے صحت کی شکایات کے بعد وائی فائی سسٹم نکال دیے۔

2005 میں آسٹریا کی میڈیکل ایسوسی ایشن نے وائی فائی کے بجائے کیبل نیٹ ورک استعمال کرنے کا مشورہ شائع کیا۔

آسٹریا سالزبرگ، جرمنی فرینکفرٹ کے مقامی محکمۂ تعلیم اور اور جرمن اساتذہ کی یونین اسکولوں میں وائی فائی کے استعمال کی مخالفت میں مشورہ دے چکے ہیں یا ان کا استعمال بند کرچکے ہیں۔

2007 کے وسط میں یورپی ماحولیات کی ایک ایجنسی نے ایک بیان جاری کیا جس میں تنبیہ کی گئی کہ جب تک سائنس کے ذریعے وائی فائی کے صحت پر اور دیگر حیات پر ہونے والے اثرات کی مزید معلومات نہیں ملتی تب تک وائی فائی و دیگر وائرلیس ذرائع مواصلات کے استعمال میں محتاط طریقہ اختیار کریں۔

سویڈن میں برق مقناطیسی حساسیت کو معذوری سمجھا جاتا ہے اور اگر آپ کو ضرورت ہو تو حکومت کی جانب سے آپ کے گھر میں اینٹی ریڈی ایشن پینٹ کیا جاتا ہے۔ نیز اسکول میں اگر ایک شخص بھی وائی فائی سے برق مقناطیسی لہروں کے منفی اثرات کی شکایت کرے تو وائی فائی کو بند کردیا جاتا ہے اور تفتیش کی جاتی ہے۔ سویڈن میں کیرولنسکا انسٹی ٹیوٹ نے 2011 میں ایک انتباہ جاری کیا جس میں درج تھا کہ سویڈن حمل زدہ خواتین وائرلیس ڈیوائسز کے استعمال سے اجتناب کریں اور دیگر استعمال کرنے والوں سے دُور رہیں جب وہ وائی فائی استعمال کررہے ہوں۔ نیز امریکا اور کینیڈا میں ریڈیو فریکوئنسی اور مائیکرو ویو شعاعوں کے سامنا کرنے کے موجودہ معیارات مکمل طور پر درست نہیں اور حمل میں موجود بچوں کے لیے حفاظتی معیارات نظر انداز کیے جاتے ہیں۔

وائی فائی سے بچاؤ

جیسا کہ بیان کیا جاچکا ہے کہ آپ اپنا وائی فائی سسٹم بند کردیں تب بھی آپ پڑوس سے آنے والی وائی فائی لہریں وصول کررہے ہوتے ہیں۔ آپ وائی فائی سے بھاگ نہیں سکتے کیوں کہ یہ اب معاشرے کا حصّہ ہے۔ یہ خصوصاً شہروں میں ہر جگہ موجود ہے۔ لہٰذا اس سے مکمل طور پر بچاؤ کم از کم شہروں میں رہنے والوں کے لیے ممکن نہیں۔ تاہم اس کا سامنا کرنے میں کمی ضرور لائی جاسکتی ہے۔

(1) وائی فائی کی شدت اور فاصلہ

کچھ مضامین وائی فائی کو غیر ضروری حد تک ایسا ثابت کرتے ہیں جیسے مائیکرو ویو اوون کام کرتا ہے۔ جب کہ حقیقت یہ ہے کہ وائی فائی کے سگنلز کی شدت مائیکرو ویو اوون سے ایک لاکھ گنا زیادہ ہوتی ہے۔ مزید یہ کہ اوون ایک حدفی ڈیوائس ہے جو ہائی وولٹیج پر اور زیادہ شدت کے ساتھ مختصر جگہ اور مختصر فاصلے پر کام کرتی ہیں۔ جب کہ وائی فائی کم وولٹیج کے ساتھ وسیع علاقے میں ہر سمت نشر ہوتی ہیں اور زیادہ فاصلے پر کام کرتی ہیں۔

چوں کہ ریڈیو لہریں دیگر برق مقناطیسی لہروں کی طرح الٹی مربع نسبت کے قانون (Inverse Square Law) پر عمل کرتی ہیں لہٰذا آپ جتنا وائی فائی ریڈیائی لہریں خارج کرنے والی اور موصول کرنے والی ڈیوائسز (وائی فائی روٹرز، ریپیٹرز، بوسٹرز، دستی کمپیوٹر، سیل فون وغیرہ) سے فاصلہ رکھیں اتنا ہی آپ ان اثرات کی شدت سے محفوظ رہ سکیں گے۔ ہر دُگنے فاصلے کے بعد آپ لہروں کی توانائی کا ایک چوتھائی حصّہ وصول کرتے ہیں۔ ایک معیاری زیرِ عمل فاصلے پر وائی فائی کی شدت عموماً اتنی کم ہوجاتی ہے کہ اس پر انسانی صحت پر ہونے والے

اثرات بہت حد تک کم ہو جاتے ہیں۔

آپ اپنا اور اپنی صحت کا تجزیہ کریں۔ اور نوٹ کریں کہ آپ برق مقناطیسی لہروں کے لیے کتنے زودِ حس ہیں اور وائی فائی کے وہ تمام اثرات کتنی شدت سے آپ محسوس کرتے ہیں جو اوپر ذکر کیے گئے ہیں۔ پھر نوٹ کریں کہ آفس یا گھر میں جہاں آپ کام کرتے ہیں وہاں سے وائی فائی روٹر کتنی دور ہے اور یقینی بنائیں کہ جس ٹیبل پر آپ کام کر رہے ہوں اس پر وائی فائی روٹر موجود نہ ہو۔ وائی فائی ٹاورز کی شدت بہت زیادہ ہوتی ہے چناچہ ان سے فاصلہ رکھنے کی کوشش کریں اور اگر آپ زیادہ برق مقناطیسی زودِ حس ہیں تو براہِ راست ان کے نیچے بیٹھنے سے اجتناب کریں۔

(2) وائی فائی کے استعمال کا دورانیہ مخصوص اور محدود کریں

چاہے آپ کام پر ہوں یا گھر پر وائی فائی کے استعمال کا دورانیہ مخصوص اور محدود کریں۔ خصوصاً کمپیوٹر نیٹ ورکنگ، کمیونی کیشن، ای بینکنگ وغیرہ سے تعلق رکھنے والے اور وہ افراد جن کے لیے روزانہ طویل دورانیے تک وائی فائی کا استعمال ضروری ہوتا ہے وہ کم از کم روٹرز اور ریپیٹرز سے فاصلے کا خیال رکھیں۔ وائی فائی یو ایس بی و دیگر وائی فائی پورٹیبل ڈیوائسز (مثلاً وائی فائی سگنلز بوسٹرز) وغیرہ کے استعمال میں احتیاط کریں۔ مثلاً وائی فائی یو ایس بی ڈیوائسز کو براہِ راست لیپ ٹاپ میں لگانے کے بجائے برقی سوئچ میں لگا کر استعمال کریں یا ایک لمبی یو ایس بی کورڈ استعمال کریں۔ لیپ ٹاپ کو گود میں رکھ کر استعمال نہ کریں۔ گھر میں رات کو روٹر آف کر دیں۔ اگر آپ کے بچے وائی فائی کے ذریعے سوشل نیٹ ورکنگ و آن لائن گیمز کھیلتے ہیں تو ان کے استعمال کے لیے اوقات مخصوص کریں اور ان کے دورانیے کو محدود کریں۔

(3) عمارتی ڈھانچے کی دھاتی پرت

کچھ معمار عمارت میں دھاتی (مثلاً) ایلومینیم کی چادر کی غیر موصل کاری (انسولیشن) کر دیتے ہیں۔ سرد علاقوں میں یہ طریقہ عمارت کو پانی سے بچانے عمارت کی اندرونی حرارت کو باہر زائل ہونے سے بچانے اور بیرونی حرارت کو اندر داخل ہونے میں مدد کرتا ہے۔ تاہم یہ ایک (مائیکل) فیراڈے کیج کی طرح کام کرتا ہے۔ فیراڈے کیج وہ شے ہے جس سے آر پار برق مقناطیسی شعاعیں نہیں گزر سکتیں۔ وائی فائی شعاعیں چوں کہ مائیکرو ویو شعاعوں کے طیفی حصّے میں ہوتی ہیں لہٰذا ایسے گھر میں وائی فائی اگر کیبل موڈیم کی صورت میں موجود ہے تو وہاں وائی فائی شعاعوں کی شدت بہت زیادہ ہوگی کیوں کہ ان لہروں کو عمارت کے پار گزرنے کے لیے راستہ کم ہوگا۔ تاہم کورڈلیس وائی فائی روٹر کو ایسے گھر میں باہر سے سگنلز نہ ملنے کے امکانات بھی اسی حد تک زیادہ ہوتے ہیں۔ چناں چہ ایسے گھر جہاں دروازے اور چھتیں دھات (مثلاً ٹین یا ایلومینیم) کی ہوں تو انھیں روٹر لگاتے وقت سگنل اور صحت دونوں اصولوں کو مدّ نظر رکھنا چاہیے۔ بعض لوگ وائی فائی کے سگنلز کو فوکس کرنے کے لیے ایلومینیم کی چادر کا سہارا لیتے ہیں انھیں بھی مذکورہ احتیاط پر غور کرنا چاہیے۔

(4) وائی فائی کے ساتھ فون استعمال کرنے میں احتیاط کریں

فون میں وائی فائی آن کرنے کے بعد یہ ضرور یاد رکھیں کہ آپ کا فون اب فون جمع وائی فائی دونوں سگنلز وصول کر رہا ہے۔ کئی افراد اسکائپ، وائبر، وغیرہ استعمال کرتے وقت براہِ راست فون کو کان سے لگاتے ہیں۔ وائی فائی کی تعددِ امواج فون سگنلز سے زیادہ لیکن تھری جی و فور جی کے قریباً مساوی ہوتی ہے۔ اس لیے وہ افراد جو وائی فائی کے ذریعے اسکائپ یا وائبر وغیرہ استعمال کرتے ہوئے فون کو براہِ راست کان سے لگاتے ہیں ان میں دماغی امراض کے امکانات بڑھ سکتے ہیں۔

لفظِ آخر کے طور پر یہاں یہ پیش کیا جانا ضروری ہے کہ اس مضمون کا مقصد قارئین میں وائی فائی کے درست استعمال اور صحت کے حوالے سے شعور کو اُجاگر کرنا ہے۔ چناچہ سب سے بہترین حکمتِ عملی ٹیکنالوجی کو ترک کر دینا نہیں بلکہ اس کے اثرات کی مکمل اور مصدقہ معلومات کے حاصل ہونے تک اس کا محتاط استعمال ہے۔ ابلاغ کے ذرائع استعمال کرنا ہر فرد کا حق ہے تاہم ہر فرد کے لیے ضروری ہے کہ وہ روزمرّہ میں استعمال ہونے والی ٹیکنالوجی سے مکمل طور پر باخبر رہے تاکہ وہ اپنی اور اپنے حلقے کے افراد کی صحت اور ماحول کے لیے ایک مثبت اور مؤثر کردار ادا کر سکے۔ اب آپ پڑوس اور اطراف سے مفت وائی فائی کے بہت سارے سگنلز وصول کرنے لگیں تو اس بات کو یاد رکھیں دنیا میں کچھ بھی مفت نہیں آپ کہیں نا کہیں اس کی قیمت ادا کر رہے ہوتے ہیں۔

اگر آپ اپنی صحت کے معاملے میں بہت حساس ہیں تو ہوسکتا ہے آیندہ آپ کسی گھر کے جائیں تو وائی فائی کا پاس ورڈ پوچھنے کی بجائے سب سے پہلے اسے آف کرنے کی درخواست کریں گے۔

اگر ایک ویب سائٹ بنانے کی بات کی جائے تو سب سے پہلے دماغ میں اس پر اُٹھنے والے اخراجات کا خیال آتا ہے کہ ڈومین نیم جو کہ قریباً ایک ہزار پاکستانی روپے کے عوض ملتا ہے۔ اس کے بعد ہوسٹنگ جو کہ پانچ ہزار روپے سے لے کر بیس یا تیس ہزار روپے تک کی بھی ہوسکتی ہے۔ اگر چہ کسی فری ہوسٹ کا بھی انتخاب کیا جاسکتا ہے لیکن اس کے مسائل الگ ہیں۔

اکثر لوگ ہم سے پوچھتے ہیں کہ کس طرح ایک ویب سائٹ اپنے ہی کمپیوٹر پر ہوسٹ کی جاسکتی ہے؟ کیا ایسا کوئی آسان حل موجود ہے کہ ہم اپنے کمپیوٹر پر ویب سائٹ تیار کر کے فوراً اسے لائیو کرسکیں؟ اگر آپ بھی اس سوال کے جواب کے متلاشی ہیں تو اس کا جواب ہے ''ہاں''۔ بہت ہی آسانی کے ساتھ اپنے کمپیوٹر پر ویب سائٹ ہوسٹ کی جاسکتی ہے۔

فرض کریں آپ ایک ویب ڈیولپر ہیں، آپ نے اپنے کسی کلائنٹ کی ویب سائٹ بنانے کا کام شروع کر رکھا ہے تو یقیناً یہ کام آپ اپنے کمپیوٹر پر سرانجام دے رہے ہوں گے۔ ویب سائٹ کو چیک کرنے کے لیے آپ نے پی سی پر لوکل سرور بنا رکھا ہوگا۔ لیکن اگر آپ کا کلائنٹ فوراً سے ویب سائٹ دیکھنے کی فرمائش کر دے تو کافی مشکل ہوسکتی ہے۔ کیونکہ اس کے لیے آپ کو سارا کام ویب سرور پر اپ لوڈ کرنا ہوگا۔ اگر یہ سہولت دستیاب ہو کہ اپنے کمپیوٹر پر موجود ویب سائٹ کسی دوسرے کو بھی دکھائی جاسکے، جو دنیا میں کہیں بھی موجود ہو تو کس قدر آسانی ہو جائے؟ کیونکہ ایک ویب سائٹ کے پیچھے ہزاروں فائلز موجود ہوتی ہیں، جنھیں اپ لوڈ کرنے کے لیے وقت درکار رہتا ہے۔

آیئے اس مضمون میں آپ کو بتاتے ہیں کہ کس طرح لوکل سرور پر موجود ویب سائٹ کو دنیا بھر میں دیکھنے کے قابل بنایا جاسکتا ہے۔ یہ طریقہ کار انتہائی سادہ اور اس قدر آسان ہے جیسے ایک دو تین کہنا۔ اگر آپ کو ویب ڈیولپمنٹ کی زیادہ معلومات نہیں تب بھی آپ باآسانی یہ کام سرانجام دے سکتے ہیں۔

ویب سرور

PHP پروگرامنگ لینگوئج کی مدد سے بنائی جانے والی ویب اپلی کیشنز کو اگر چہ ہر معروف ویب سرور کے ساتھ استعمال کیا جاسکتا ہے لیکن عام طور پر اس کے لئے Apache ویب سرور کا انتخاب کیا جاتا ہے جو کہ مفت دستیاب ہے۔ اپاچی ویب سرور کا کام صارفین کی طرف سے درخواستیں موصول کرنا اور ان کا جواب دینا ہوتا ہے۔ مثلاً جب کوئی صارف براؤزر میں کسی ویب پیج وغیرہ کا ایڈریس ٹائپ کرتا ہے تو براؤزر یہ درخواست ویب سرور کے پاس بھیجتا ہے۔ اس ویب سرور پر یہ درخواست اپاچی سافٹ ویئر وصول کرتا ہے اور پھر صارف کی درخواست کے مطابق ڈسک سے مطلوبہ فائل تلاش کر کے بھیجتا ہے۔ صارف کی یہ درخواست ایسے ویب پیج کے لیے بھی ہوسکتی ہے جو پی ایچ پی کی مدد سے بنایا گیا ہو اور اس ویب پیج میں MySQL ڈیٹا بیس سے کچھ ریکارڈز حاصل کر کے شامل کیے گئے ہوں۔

ویب ہوسٹنگ اکاؤنٹ اس لیے حاصل کیا جاتا ہے تاکہ ویب سائٹ یا ویب اپلی کیشن لوگوں کے استعمال کے لیے اپ لوڈ کی جاسکے۔ لیکن ویب اپلی کیشن کی ڈیولپمنٹ کے لیے ہوسٹنگ اکاؤنٹ کا استعمال کچھ زیادہ فائدہ مند نہیں رہتا۔ اس لیے کہ پروگرامنگ کے دوران کوڈ میں تبدیلیاں کرتے ہوئے

ایپلی کیشن کو مسلسل ٹیسٹ کرنا پڑتا ہے۔ ہر تبدیلی کے بعد کوڈ کی فائل اپ لوڈ کرنا اور پھر براؤزر میں ٹیسٹ کرنا دقت طلب کام ہے۔ اس کے علاوہ ہوسٹنگ اکاؤنٹ استعمال کرتے ہوئے ویب ڈیولپمنٹ کے لیے انٹرنیٹ کنکشن بھی ہر وقت درکار ہوتا ہے۔

لوکل سرور

ڈیولپرز اپنے ذاتی کمپیوٹر پر وہ تمام ٹولز اور سافٹ ویئرز انسٹال کر لیتے ہیں جن کی مدد سے ہوسٹنگ اکاؤنٹ اور انٹرنیٹ کنکشن کے بغیر ویب ڈیولپمنٹ کی جا سکے۔ چنانچہ ویب ایپلی کیشن ڈیولپمنٹ کے لیے درج ذیل سافٹ ویئر پیکیجز کمپیوٹر پر انسٹال کرنا ضروری ہیں:

خودکار طریقے سے ویب پیجز بنانے کے لیے PHP پروگرامنگ لینگوئج۔

ویب ایپلی کیشنز کا ڈیٹا محفوظ کرنے کے لیے MySQL ڈیٹا بیس سسٹم۔

براؤزر میں ویب ایپلی کیشن چلانے کے لیے Apache ویب سرور۔

کم سے کم SQL کوڈ لکھتے ہوئے ڈیٹابیسز پر کام کرنے کے لیے phpMyAdmin ویب ایپلی کیشن۔

ایپلی کیشن کی رفتار ٹیسٹ کرنے کے لیے webGrind یا اس جیسا کوئی دوسرا ٹول۔

لوکل ویب سرور بنانے کے لیے یہ تمام سافٹ ویئرز انسٹال کرنا ضروری ہوتے ہیں۔ اس کام کو آسان بنانے کے لیے "ویمپ سرور" موجود ہے۔ WampServer درج بالا تمام سافٹ ویئرز ایک ہی انسٹالیشن پیکیج کی صورت میں مہیا کر دیتا ہے۔ اگر آپ WampServer یا اس جیسا کوئی دوسرا ٹول استعمال نہیں کریں گے تو آپ کو یہ تمام سافٹ ویئرز الگ الگ ڈاؤن لوڈ کر کے انسٹال کرنا پڑیں گے۔

ویمپ سرور کی انسٹالیشن دیگر پروگرامز کی انسٹالیشن کی طرح ہی چند کلکس کی متقاضی ہے۔ اس کی انسٹالیشن سے با آسانی کمپیوٹر پر ایک لوکل ویب سرور بنایا جا سکتا ہے۔ ویمپ درج ذیل ربط سے ڈاؤن لوڈ کیا جا سکتا ہے:

www.wampserver.com/en

ویمپ کو انسٹال کرنے کے بعد چلائیں، اس کی تمام سروسز چلنے کے بعد سسٹم ٹرے میں موجود اس کا آئی کن ہرے رنگ کا ہو جائے گا۔ اگر آپ کے پاس اس کا آئی کن ہرا نہ ہو تو اس کا مطلب ہے کہ اس کی کوئی سروس نہیں چل پا رہی۔ اس کے لیے اس کے آئی کن پر کلک کر کے تمام سروسز کو چلا دیں۔ اکثر یہ بھی دیکھنے میں آیا کہ اگر آپ اسکائپ استعمال کر رہے ہوں تو ویمپ نہیں چل پاتا، کیونکہ دونوں کام کرنے کے لیے ایک ہی پورٹ استعمال کر رہے ہوتے ہیں۔ اس لیے اسکائپ کو بند کر دینے سے ویمپ صحیح کام کرنا شروع کر دیتا ہے۔

ویمپ انسٹالیشن کے دوران یہ پوچھتا ہے کہ آپ کس لوکیشن پر سرور بنانا چاہتے ہیں۔ عموماً یہ سی ڈرائیو میں wamp کے نام سے اپنا فولڈر بناتا ہے۔ اس طرح C:\wamp\www کے مقام پر آپ اپنی ویب سائٹ کی فائلز رکھ انھیں لوکل سرور میں ملاحظہ کر سکتے ہیں۔ تاہم آپ اس پاتھ کو اپنی منشاء کے مطابق تبدیل بھی کر سکتے ہیں۔

ویمپ کی انسٹالیشن کی درستگی جانچنے کے لیے ویب براؤزر میں localhost لکھ کر انٹر پریس کریں۔ Localhost کا مطلب یہ ہے کہ ہم بذریعہ نیٹ ورک اپنے ہی کمپیوٹر تک رسائی حاصل کر رہے ہیں۔ آپ براؤزر میں Localhost لکھنے کی بجائے 127.0.0.1 بھی لکھ سکتے ہیں جو کہ زیادہ تر کمپیوٹرز کا Loopback ایڈریس ہوتا ہے۔

لوکل ہوسٹ کے ربط پر لوکل سرور کے بارے میں ساری معلومات موجود ہو گی۔ یہ صفحہ کھلنے کا مطلب ہے کہ آپ نے درست طریقہ سے لوکل سرور بنا لیا ہے۔ اب اگر آپ چاہیں تو localhost کی جگہ اپنے سسٹم کا آئی پی ایڈریس استعمال کرتے ہوئے نیٹ ورک پر موجود کسی بھی دوسرے سسٹم سے اپنے لوکل سرور پر موجود ویب سائٹ کو دیکھ سکتے ہیں۔

WAMPSERVER Homepage
localhost
WampServer
Version 2.5 Version Française

Server Configuration
Apache Version : 2.4.9 - Documentation
PHP Version : 5.5.12 - Documentation
Server Software: Apache/2.4.9 (Win64) PHP/5.5.12
Loaded Extensions : apache2handler, bcmath, bz2, calendar, com_dotnet, Core, ctype, curl, date, dom, ereg, exif, fileinfo, filter, ftp, gd, gettext, gmp, hash, iconv, imap, json, libxml, mbstring, mcrypt, mhash, mysql, mysqli, mysqlnd, odbc, openssl, pcre, PDO, pdo_mysql, pdo_sqlite, Phar, Reflection, session, shmop, SimpleXML, soap, sockets, SPL, sqlite3, standard, tokenizer, wddx, xdebug, xml, xmlreader, xmlrpc, xmlwriter, xsl, zip, zlib
MySQL Version : 5.6.17 - Documentation

Tools: phpinfo(), phpmyadmin
Your Projects: fb, wordpress
Your Aliases: phpmyadmin, phpsysinfo, sqlbuddy, webgrind

لوکل سرور کو آن لائن کرنا

لوکل سرور پر موجود ویب سائٹ کو لائیو کرنے کے لیے لوکل سرور کو گلوبلی آن لائن کر دینا، نہ صرف ویب سائٹ کو فوراً دنیا میں کہیں بھی دیکھنے کے قابل بنا دیتا ہے بلکہ آپ کسی قسم کی اپ لوڈنگ سے بھی بچ جاتے ہیں۔ یہ اس طرح بھی فائدے مند ہوسکتا ہے کہ آپ عارضی طور پر کوئی ویب سائٹ بنانا چاہیں، یا مستقل طور پر اپنی ویب سائٹ اپنے کمپیوٹر پر ہوسٹ کرنا چاہیں یا مقصد فائل شیئرنگ ہو تمام صورتوں میں اپنے کمپیوٹر اور انٹرنیٹ کی بدولت لوکل سرور پر موجود ویب سائٹ کو دنیا بھر میں دیکھنے کے قابل بنا جاسکتا ہے۔

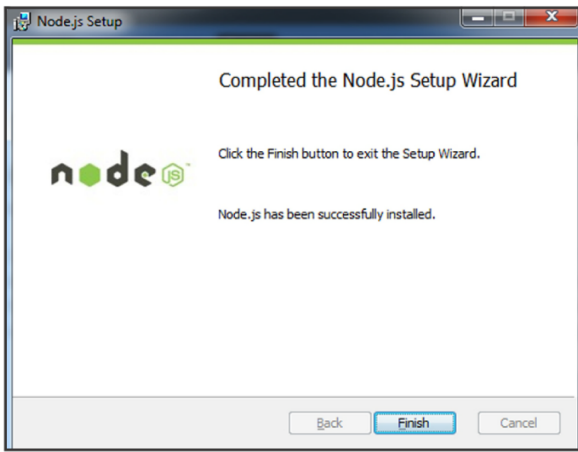
لوکل ٹنل (Local Tunnel)

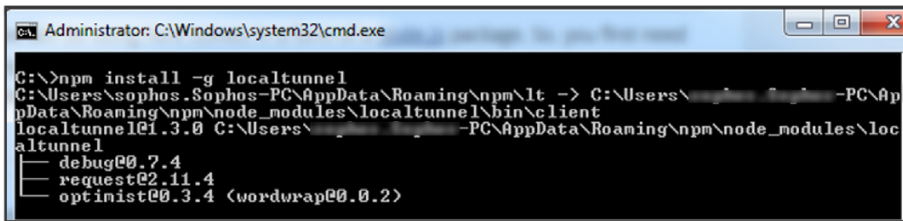
لوکل سرور کو ویب سرور میں بدلنے کے لیے ہمیں جو ٹول چاہیے وہ ہے ''لوکل ٹنل''۔ یہ ٹول ایک پراکسی کے ذریعے ہمارے لوکل سرور تک ایک ''سرنگ'' بناتے ہوئے اسے دنیا میں کہیں بھی دیکھنے کے قابل بنا دیتا ہے۔

یاد رہے کہ آپ کی ویب سائٹ تب ہی دیکھی جا سکے گی جب آپ کا کمپیوٹر نہ صرف آن ہوگا بلکہ اس پر انٹرنیٹ بھی چل رہا ہوگا۔ کمپیوٹر کے آف ہونے یا انٹرنیٹ کے دستیاب نہ ہونے کی صورت میں ویب سائٹ نیٹ ورک کے علاوہ کہیں نہیں دیکھی جا سکے گی۔

لوکل ٹنل کی انسٹالیشن

لوکل ٹنل Node.js پیکیج میں فراہم کیا جاتا ہے۔ اس لیے پہلے آپ کو ''نوڈ ڈاٹ جے ایس'' درج ذیل ربط سے ڈاؤن لوڈ کرنا ہوگا:

nodejs.org/download

یہ پیکیج ساڑھے پانچ ایم بی سائز کا حامل ہے، جسے ڈاؤن لوڈ کرنا کوئی مشکل کام نہیں۔ نوڈ ونڈوز کے علاوہ میک اور لینکس صارفین کے لیے بھی بالکل مفت دستیاب ہے۔ ڈیویلپرز کے لیے اس کا سورس کوڈ بھی اسی صفحے پر موجود ہے۔

اس کی انسٹالیشن بھی انتہائی سادہ سی ہے۔ ڈاؤن لوڈ کی گئی اس کی فائل پر ڈبل کلک کرکے چلائیں، چند لمحوں میں اس کی انسٹالیشن مکمل ہوجائے گی۔

نوڈ ڈاٹ جے ایس کی انسٹالیشن کے بعد ٹرمنل یا کمانڈ پرامپٹ کھول کر اس میں درج ذیل کمانڈ ٹائپ کریں:

npm install -g localtunnel

یہ کمانڈ لوکل ٹنل کو دنیا بھر میں کہیں بھی قابل رسائی بنانے کے لیے انسٹال کر دے گی۔ انسٹالیشن مکمل ہونے کے بعد دیگر کام کرنے کے لیے اس کی کمانڈ ''ایل ٹی'' (lt) استعمال کرنا ہوگی۔

مثلاً کمانڈ ٹیسٹ کرنے کے لیے اور ٹنل کی درست کنفگریشن کو آزمانے کے لیے ایک آزمائشی کمانڈ ٹائپ کرتے ہیں:

lt - -version

ایل ٹی کے بعد اسپیس دے کر دو منفی کے نشان اور آگے ورژن لکھ کر انٹر پریس کریں تو نتیجے کے طور پر اسے لوکل ٹنل کا ورژن دکھانا چاہیے۔ جیسا کہ آپ

```
Administrator: C:\Windows\system32\cmd.exe

C:\>lt --version
1.3.0

C:\>
```

تصویر میں دیکھ سکتے ہیں اس نے ورژن 1.3.0 دکھایا ہے۔ اگر آپ کے پاس ورژن نمبر نہ دکھائے تو دوبارہ کوشش کریں اور دھیان سے کمانڈ بالکل درست طریقے سے ٹائپ کریں۔

کسی قسم کی مدد کے لیے آپ lt - - help کی کمانڈ استعمال کر سکتے ہیں۔ یہ کمانڈ لوکل ٹنل پر دستیاب آپشن اور انھیں استعمال کرنے کا طریقہ بتا دیتی ہے۔

لوکل ٹنل کا استعمال

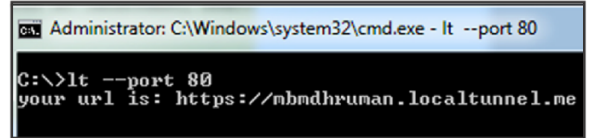
آپ لوکل سرور پہلے ہی بنا چکے ہیں اس کے بعد نوڈ جے ایس کی بھی انسٹالیشن ہو چکی ہے تو آیئے دیکھتے ہیں کہ لوکل ٹنل کو کیسے استعمال کیا جاتا ہے۔ ہمیں امید ہے کہ آپ نے لوکل سرور پر بنیادی قسم کی کوئی ویب سائٹ چاہے وہ ایک ہی صفحے کی ہی کیوں نہ ہو بنا لی ہوگی تاکہ لوکل ٹنل کی آزمائش ہو سکے۔ آسانی کے لیے آپ لوکل سرور پر ورڈپریس بھی انسٹال کر سکتے ہیں۔

لوکل سرور پر موجود اپنی ویب سائٹ کے لیے ایک گلوبل ربط حاصل کرنے کے لیے کمانڈ پرامپٹ پر یہ کمانڈ چلانی ہوگی:

lt - -port 80

(ایل ٹی اسپیس دو مائنس نشان پورٹ اسپیس 80)

```
Administrator: C:\Windows\system32\cmd.exe - lt  --port 80

C:\>lt --port 80
your url is: https://mbmdhruman.localtunnel.me
```

یہ کمانڈ اپنا کام پورا کرتے ہی آپ کے لوکل سرور کے لیے ایک بے ترتیب سا سب ڈومین نیم بنا دے گی۔ یعنی اگر آپ کا لوکل ویب سرور چل رہا ہو تو اس ربط کے ذریعے اب آپ کی لوکل ویب سائٹ کو دنیا بھر میں کہیں بھی دیکھا جا سکتا ہے۔ اگر آپ کو یہ بے ترتیب سا نام پسند نہیں اور آپ اپنی پسند کا سب ڈومین حاصل کرنا چاہتے ہیں تو اس کے لیے الگ کمانڈ استعمال کرنی ہوگی۔ مثلاً:

```
Administrator: C:\Windows\system32\cmd.exe - lt  --port 80 --subdomain comp

C:\>lt --port 80 --subdomain computingpk
your url is: https://computingpk.localtunnel.me
```

lt - -port 80 - -subdomain computingpk

یہ کمانڈ آپ کی پسند کا سب ڈومین حاصل کرنے کی کوشش کرے گی۔ اگر وہ سب ڈومین دستیاب ہوا تو فوراً ہی آپ کو دے دیا جائے گا۔ اب ایک بے ترتیب ربط یاد رکھنے کی ضرورت نہیں بلکہ اپنے اس سب ڈومین کی مدد سے اپنے

لوکل سرور پر موجود ویب سائٹ کہیں سے بھی دیکھی جا سکتی ہے۔

لوکل ٹنل ورچوئل ہوسٹ کو بھی سپورٹ کرتا ہے۔ جب lt - -port 80 کمانڈ استعمال کی جاتی ہے تو لوکل ٹنل بطور ڈیفالٹ localhost کو کنیکٹ کرنے کے لیے منتخب کر لیتا ہے۔ اگر آپ نے ورچوئل ہوسٹ بنا رکھا ہے اور فرض کرتے ہیں اس کا نام computingpk.dev ہے تو آپ لوکل ٹنل کو لوکل ہوسٹ کی بجائے ورچوئل ہوسٹ سے بھی کنیکٹ کر سکتے ہیں۔ اس کے لیے - - local - - host کے پیرامیٹرز استعمال کرنا ہوں گے۔

اب جو کمانڈ ٹائپ کرنا ہے وہ کچھ یوں ہوگی:

lt --port 80 --subdomain computingpk

--local--host computingpk.dev

ویب ڈیویلپرز کے لیے "لوکل ٹنل" کا موجود ہونا ایک نعمت سے کم نہیں۔ جیسا کہ آپ نے اس مضمون میں پڑھا اسے کنفیگر کرنا بھی انتہائی آسان ہے۔

سکیوریٹی خطرات

لوکل ٹنل چونکہ محفوظ https پروٹوکول استعمال کرتا ہے اس لیے اس میں سکیوریٹی خطرات کا اندیشہ معدوم ہو جاتا ہے۔ کمانڈ پرامپٹ کے بند ہوتے ہی آپ کے کمپیوٹر تک "سرنگ" کے ذریعے بنائے گئے رابطے منقطع کر دیے جاتے ہیں۔ جب آپ اپنی ویب سائٹ آف لائن کرنا چاہیں، لوکل ویب سرور کو بھی آف کر سکتے ہیں۔

ونڈوز میں پوشیدہ 10 خفیہ ٹولز

جو آپ کے کمپیوٹر کو صحت مند رکھنے میں معاون ہیں

آپ چاہے ونڈوز 8، ونڈوز 7 یا ونڈوز کا پرانا ورژن استعمال کر رہے ہوں، اس میں بہت سے سسٹم ٹولز ایسے ہوتے ہیں جو بہت کام کے ہوتے ہیں مگر وہ عام نظروں سے اوجھل رہتے ہیں۔ ان میں سے کچھ تو اسٹارٹ مینو میں کہیں دفن ہوتے ہیں جبکہ کچھ کو مخصوص کمانڈز کے ذریعے چلایا جاسکتا ہے۔

اگر آپ کو ان ٹولز کے نام معلوم ہوں تو ان میں سے بہت سے ٹولز کو آسانی سے چلایا جا سکتا ہے۔ بس اسٹارٹ مینو کو کھولیں یا اسٹارٹ اسکرین کھول کر پروگرام کا نام لکھ کر سرچ کریں اور کی بورڈ سے انٹر کا بٹن دبائیں۔ ونڈوز 8 میں پہلے آپ سیٹنگز کیٹیگری میں سے سرچ اسکرین سلیکٹ کرلیں۔

ونڈوز میموری ڈائی گنوسٹک

ونڈوز کے اندر میموری چیک کرنے کا ایک ٹول بھی موجود ہوتا ہے جس کی مدد میموری کے نقائص کا پتا چلایا جا سکتا ہے۔ یہ ٹول بھی اسی طرح کام کرتا ہے جیسے مشہور MemTest86 پروگرام کام کرتا تھا۔ اگر آپ اپنے کمپیوٹر کی میموری کو نقائص کے حوالے سے چیک کرنا چاہیں تو آپ کو تھرڈ پارٹی پروگرام کرنے کی ضرورت نہیں، بس Windows Memory Diagnostic ٹول استعمال کریں۔ اگر ونڈوز کو محسوس ہو کہ میموری میں کوئی مسئلہ ہے تو وہ یہ ٹول خود ہی چلا کر آپ کو آپشن منتخب کرنے کا کہتی ہے۔ لیکن آپ اس ٹول کو خود بھی چلا سکتے ہیں۔ اسٹارٹ مینو کھولیں اور سرچ میں Memory لکھیں۔ ظاہر ہونے والے آپشنز میں یہ ٹول بھی موجود ہوگا۔ اس پر کلک کر کے اسے چلائیں۔ اس میں دو آپشنز دیئے گئے ہیں۔ اوّل Restart Now and check for problems جبکہ دوسرا Check for problems the next time I start my computer۔ پہلا آپشن منتخب کرنے کی صورت میں کمپیوٹر فوراً ری اسٹارٹ ہوجائے گا اور یہ ٹول میموری میں سے ایررز تلاش کرنا شروع کردے گا۔ جبکہ دوسرا آپشن منتخب کرنے کی صورت میں آپ جب خود کمپیوٹر ری اسٹارٹ کریں گے تو یہ ٹول میموری کو اسکین کرے گا۔

ریسورس مونیٹر

ریسورس مونیٹر کی مدد سے آپ اپنے سسٹم کے تمام ریسورسز کو چیک کر سکتے ہیں، جو سسٹم استعمال کر رہا ہے۔ یہ ٹول آپ کو کمپیوٹر کے سی پی یو، ڈسک، نیٹ ورک اور میموری گرافکس کے حوالے سے ہر طرح کی تفصیل سے آگاہ کرتا ہے۔

اس پروگرام سے آپ دیکھ سکتے ہیں کہ کون سا پروگرام آپ کی ڈسک یا نیٹ ورک کو زیادہ استعمال کر رہا ہے۔ اس سے یہ بھی پتا چل جائے گا کہ کون سا پروسس انٹرنیٹ کے کس ایڈریس سے رابطہ کر رہا ہے۔ ریسورس مانیٹر پروگرام ٹاسک مینیجر سے زیادہ تفصیلی رپورٹ کے ساتھ نتائج ظاہر کرتا ہے۔ یہ ٹول اس وقت خاص طور پر مفید ثابت ہوتا ہے جب کمپیوٹر کی سست رفتاری کی وجہ معلوم نہ ہو پا رہی ہو۔ اس کی مدد سے آپ با آسانی جان سکتے ہیں کہ

آیا کوئی پروگرام سی پی یو کا بے دریغ استعمال کر رہا ہے یا ڈسک پر دھڑا دھڑ ڈیٹا لکھ کر اسے مصروف رکھے ہوئے ہے۔

ریسورس مانیٹر کو ٹاسک مینیجر کی مدد سے کھولا جا سکتا ہے۔ ٹاسک مینیجر کھول کر پرفارمنس کی ٹیب کھول لیں اور ریسوریس مانیٹر سلیکٹ کر لیں۔ اس کے علاوہ ریسورس مانیٹر اسٹارٹ مینو میں سرچ کر کے بھی چلایا جا سکتا ہے۔

پرفارمنس مونیٹر

پرفارمنس مونیٹر ایپلی کیشن کی مدد سے آپ کمپیوٹر کی مجموعی یا کسی حصے (مثلاً ہارڈ ڈسک) کی انفرادی رپورٹ دیکھ سکتے ہیں۔ اس کے ذریعے مختلف اوقات میں کمپیوٹر کی کارکردگی کی رپورٹ بھی تیار کی جا سکتی ہے۔ یہ بھی دیکھا جا سکتا ہے کہ سسٹم میں ہونے والی کسی تبدیلی سے پرفارمنس میں کیا تبدیلی ہوئی۔ یہ ٹول نیٹ ورک پر موجود دوسرے کمپیوٹرز کی کارکردگی جانچنے کے لئے بھی استعمال کیا جا سکتا ہے۔ لیکن اس کے لئے نیٹ ورک پر موجود کمپیوٹر تک ایڈمنسٹریٹر لیول کے رائٹس کے ساتھ رسائی درکار ہو گی۔

کمپیوٹر مینجمنٹ اینڈ ایڈمنسٹریٹیو ٹولز

پرفارمنس مانیٹر اصل میں مائیکروسافٹ مینجمنٹ کنسول ٹولز کا ہی ایک حصہ ہے۔ اس طرح کے بہت سے ٹولز Administrative Tools کے فولڈر میں ہوتے ہیں۔ تاہم یہ اس فولڈر میں الگ الگ موجود ہوتے ہیں۔ ان ٹولز کو ایک ہی جگہ کمپیوٹر مینجمنٹ (Computer management) میں استعمال کیا جا سکتا ہے۔ کمپیوٹر مینجمنٹ کھولنے کے لئے مائی کمپیوٹر پر رائٹ کلک کریں اور Computer Management کے آپشن پر کلک کریں۔ اس میں درج ذیل ٹولز موجود ہوتے ہیں:

ٹاسک شیڈولر

اس کے ذریعے کسی پروگرام کو دن کے کسی مخصوص وقت پر خودکار طور پر چلایا جا سکتا ہے۔ مثلاً ٹاسک شیڈولر کے ذریعے آپ رات 12 بجے کمپیوٹر کو خودکار طور پر شٹ ڈاؤن کر سکتے ہیں۔

ایونٹ ویوور

ٹربل شوٹنگ کے دوران لوگ اس اہم ٹول کو اکثر بھول جاتے ہیں۔ ونڈوز میں پیش آنے والے ہر واقعے، چاہے وہ کوئی ایرر ہو یا کسی سافٹ ویئر کی انسٹالیشن، سسٹم کریش ہونے کا واقعہ ہو یا کسی ڈیوائس کی خرابی، ان سب کے بارے میں تفصیل محفوظ کی جاتی ہے۔ یہ تفصیل ایونٹ ویوور کے ذریعے دیکھی جا سکتی ہے۔ بعض اینٹی وائرسز کے لاگز بھی ایونٹ ویوور میں دیکھے جا سکتے ہیں۔

شیئرڈ فولڈر

یہ ایک انٹرفیس ہے جہاں آپ کے کمپیوٹر سے نیٹ ورک پر شیئر کئے ہوئے تمام فولڈرز دیکھے جا سکتے ہیں۔ اسی انٹرفیس سے شیئر کئے گئے فولڈرز کی شیئرنگ کا خاتمہ کیا جا سکتا ہے یا شیئر فولڈر کی سکیوریٹی میں تبدیلی کی جا سکتی ہے۔

ڈیوائس مینیجر

ڈیوائس مینیجر کی مدد سے کمپیوٹر سے جڑی تمام ڈیوائسز کو دیکھا جا سکتا

ہے، ان کو غیر فعال یا ڈس ایبل کیا جا سکتا ہے، ڈیوائسز کے ڈرائیورز کو اپ ڈیٹ، ڈیلیٹ یا رول بیک بھی کیا جاسکتا ہے۔

ڈسک مینجمنٹ

یہ ونڈوز میں شامل پہلے سے پارٹیشن مینیجر ہے۔ اس کی مدد سے بغیر کوئی دوسرا سافٹ ویئر ڈاؤن لوڈ کیے پارٹیشن وغیرہ بنائی جاسکتی ہیں، ری سائز کی جاسکتی ہے، اُن کا سائز دیکھا جاسکے گا۔ اس کے ذریعے کسی پارٹیشن کا ڈرائیو لیٹر بھی تبدیل کیا جاسکتا ہے۔ کمپیوٹر سے ساتھ لگی ماس اسٹوریج ڈیوائسز اور آپٹیکل ڈرائیوز کی تفصیل بھی اس میں نظر آرہی ہوتی ہے۔ ایک دلچسپ چیز یہاں یہ بھی کی جاسکتی ہے کہ کسی پارٹیشن کا ڈرائیو لیٹر ختم کر کے اسے مائی کمپیوٹر سے غائب کیا جاسکتا ہے۔

سروسز

یہ ایک انٹرفیس ہے جس میں ونڈوز میں پسِ پردہ چلنے والی سروسز کو دیکھا جا سکتا ہے۔ Administrative Tools فولڈر میں چند دوسری مفید یوٹیلیٹی بھی شامل ہوتی ہیں، جیسے کہ ونڈوز فائر وال اور ایڈوانسڈ سکیوریٹی ایپلی کیشن کی مدد سے فائر وال کی سیٹنگ کی جاسکتی ہے۔

ایڈوانسڈ یوزر اکاؤنٹس ٹول

ونڈوز میں User Accounts نامی ایک یوٹیلیٹی پوشیدہ ہوتی ہے جس میں کئی آپشنز ایسے موجود ہیں جو ونڈوز کے ظاہری انٹرفیس پر موجود نہیں ہوتے۔

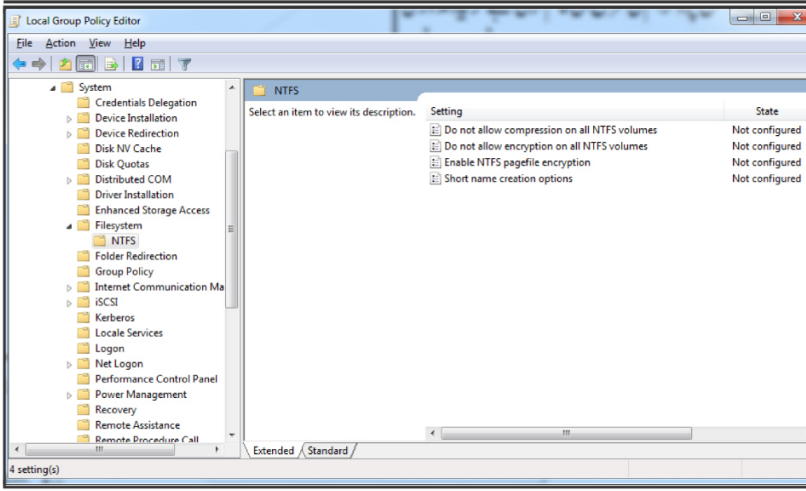
User Accounts
Users Advanced
Passwords
You can manage the passwords you have stored on this computer
Manage Passwords
Advanced user management
Local Users and Groups can be used to perform advanced user management tasks.
Advanced
Secure logon
For added security, you can require users to press Ctrl+Alt+Delete before logging on. This guarantees that the authentic Windows logon prompt appears, protecting the system from programs that mimic a logon to retrieve password information.
Require users to press Ctrl+Alt+Delete

اس ٹول کو چلانے کے لئے WinKey+R دبا کر Run باکس کو اوپن کر لیں۔ اب رن ڈائیلاگ باکس میں netplwiz یا پھر userpasswords2 ٹائپ کر کے انٹر کا بٹن دبا دیں۔ یاد رہے کہ یہ ٹپ ونڈوز ایکس پی سے جدید ورژنز کے لیے ہے۔

اس ونڈو میں ایک شارٹ کٹ Local Users and Groups ٹول کو لانچ کرنے کے لیے بھی ہوتا ہے، اس ٹول کی مدد سے یوزر مینجمنٹ کے دوسرے ٹاسک بھی سرانجام دیئے جاسکتے ہیں۔

یوزر اکاؤنٹس ٹول میں Advanced کے ٹیب میں Manage Passwords کا بٹن موجود ہے۔ اس پر کلک کرنے سے Windows Vault کھلتا ہے جس میں نیٹ ورک کمپیوٹرز کو ایکسس کرنے کے لئے استعمال کئے گئے تمام یوزر نیم اور پاس ورڈز محفوظ ہوتے ہیں۔ آپ ان کا بیک اپ بھی لے سکتے ہیں اور پہلے سے موجود بیک اپ سے واپس بحال بھی کر سکتے ہیں۔ جبکہ پاس ورڈ ڈیلیٹ بھی کئے جاسکتے ہیں۔

ڈسک کلین اپ

ونڈوز کی ڈسک کلین اپ یوٹیلیٹی اگرچہ اتنی پوشیدہ نہیں ہوتی جتنا کہ باقی ٹولز ہوتے ہیں، تاہم اس کے باوجود کئی مبتدیوں کو اس کے بارے میں علم نہیں ہوتا۔ یہ یوٹیلیٹی آپ کے کمپیوٹر کی اُن فائلوں کی تلاش میں رہتی ہے جن کو ڈیلیٹ کر کے صارفین ہارڈ ڈسک پر مزید جگہ بنا سکتے ہیں۔ ونڈوز کی عارضی فائلیں، میموری ڈمپ (dump)، پرانے سسٹم ری اسٹور پوائنٹس اور سسٹم کی اپ گریڈنگ کے دوران پرانی فائلیں اس یوٹیلیٹی کا خاص ہدف ہوتی ہیں جن کو تلاش کر کے یہ یوٹیلیٹی ڈیلیٹ کرنے کے لیے پیش کر دیتی ہے۔ ڈسک کلین اَپ دوسرے

پروفیشنل پروگرام کی طرح ہی کام کرتی ہے مگر یہ ونڈوز کی جانب سے مفت میں دستیاب ہے۔ ایڈوانس صارفین CCleaner کے استعمال کو ترجیح دیتے ہیں مگر ڈسک کلین اپ یوٹیلیٹی یہی کام کافی عمدگی اور آسانی سے کرتی ہے۔ اسے چلانے کے لیے اسٹارٹ مینو سے اسے تلاش کرلیں ورنہ ضرورت کے وقت یہ خود بخود بھی ظاہر ہوتی ہی رہتی ہے۔

گروپ پالیسی ایڈیٹر

یہ ٹول ونڈوز کے پروفیشنل یا الٹی میٹ ایڈیشن کے ساتھ دستیاب ہوتا ہے، اسٹینڈرڈ اور ہوم ایڈیشن میں یہ موجود نہیں ہوتا۔ بنیادی طور پر یہ یوٹیلیٹی سسٹم ایڈمنسٹریٹر کے کام کی ہے جس کی مدد سے وہ اپنے نیٹ ورک پر موجود کمپیوٹرز کی سیکیوریٹی کو سخت بنانے کے ساتھ ساتھ ان میں ایسی تبدیلیاں بھی کرسکتے ہیں جو عام طور پر ممکن نہیں ہوتیں۔ مثال کے طور پر گروپ پالیسی کے ذریعے یو ایس بی کا آٹو رن فیچر غیر فعال کیا جاسکتا ہے، سسٹم ٹرے میں نظر آنے والی گھڑی کو غائب کیا جاسکتا ہے۔

لوکل گروپ پالیسی ایڈیٹر میں بھی کچھ ایسی سیٹنگز ہوتی ہیں جس میں اوسط درجے کے صارف کی دلچسپی ہوتی ہے۔ مثال کے طور پر ونڈوز 8 میں گروپ پالیسی ایڈیٹر کی مدد سے لاک اسکرین کو ڈس ایبل کیا جاسکتا ہے اور براہ راست لاگ ان اسکرین تک جایا جاسکتا ہے۔

اسے کھولنے کے لیے اسٹارٹ مینو میں یا اسٹارٹ سکرین میں gpedit.msc لکھ کر انٹر کردیں۔

رجسٹری ایڈیٹر

رجسٹری ایڈیٹر کے بارے میں ہر کوئی جانتا ہے مگر یہ یوٹیلیٹی پھر بھی پوشیدہ ہے۔ مائیکروسافٹ نے اسٹارٹ مینو میں اس کا کوئی شارٹ کٹ نہیں بنایا۔ اسے چلانے کے لیے Run یا اسٹارٹ اسکرین میں regedit لکھ کر انٹر کردیں۔

رجسٹری ایڈیٹر کی مدد سے اسی طرح کے کام بھی کیے جاسکتے ہیں جو گروپ پالیسی ایڈیٹر کی مدد سے کیے جاسکتے ہیں۔ مثال کے طور پر ونڈوز 8 کے صارفین ونڈو کے اسٹینڈرڈ ایڈیشن میں گروپ پالیسی ایڈیٹر کی مدد سے لاک اسکرین کو غیر فعال یا ڈس ایبل نہیں کیا جاسکتا مگر رجسٹری ایڈیٹر کی مدد سے اسے ڈس ایبل کیا جاسکتا ہے۔ یاد رہے کہ رجسٹری ایڈیٹر میں کوئی بھی تبدیلی انتہائی احتیاط سے کرنی چاہئے۔ بصورت دیگر ونڈوز میں زبردست خرابی پیدا ہوسکتی ہے۔

سسٹم کنفگریشن یوٹیلیٹی

سسٹم کنفگریشن ونڈو بھی ایک اہم ٹول ہے۔ اس کے بارے میں بھی کافی لوگ جانتے ہیں۔ ونڈوز ایکس پی کے دور میں یہ ایک اسٹارٹ اپ مینیجر پروگرام کی حیثیت رکھتا تھا۔ لیکن اب ونڈوز کے جدید ورژنز میں اس یوٹیلیٹی کو بھی جدید سہولیات سے مزین کردیا گیا ہے۔ اب اس کے ذریعے نہ صرف آپ اسٹارٹ اپ پروگرامز (جو ونڈوز کے اسٹارٹ ہوتے ہی چل پڑتے ہیں) کی فہرست کی تدوین کرسکتے ہیں بلکہ آپریٹنگ سسٹم کے بوٹ آپشنز سمیت درجنوں دیگر تبدیلیاں کرسکتے ہیں۔ آپریٹنگ سسٹم کے بوٹ آپشنز میں تبدیلی والا فیچر اس وقت زیادہ کام آتا ہے جب آپ کے کمپیوٹر پر بہت سے آپریٹنگ سسٹم انسٹال ہوں۔ اس ٹول کو لانچ کرنے کے لیے رن کے ڈائیلاگ باکس میں msconfig لکھ کر انٹر پریس کردیں۔

سسٹم انفارمیشن

سسٹم انفارمیشن یوٹیلیٹی کی مدد سے کمپیوٹر کی تمام معلومات کو دیکھا جاسکتا ہے۔ ان معلومات میں ماڈل نمبر، سی ڈی روم ڈرائیو اور دوسری منسلک ڈیوائسز کی معلومات بھی دکھائی جاتی ہے۔ یہ پروگرام تھرڈ پارٹی پروگرام Speccy کی طرح بہت زیادہ تفصیل میں تو نتائج نہیں دِکھاتا مگر پھر بھی بہت سی اہم معلومات ظاہر کردیتا ہے۔ اسٹارٹ مینو میں System Information لکھ کر اس پروگرام کو سرچ کرکے چلایا جاسکتا ہے۔

④ اشتہارات خود بخود کھل جاتے ہیں

انٹرنیٹ استعمال کرنے والے اکثر مبتدی حضرات کو یہ شکایت رہتی ہے کہ انٹرنیٹ براؤزنگ اور بعض اوقات بغیر انٹرنیٹ کے بھی ان کے کمپیوٹر پر عجیب و غریب (کئی کیسز میں غیر اخلاقی) اشتہارات ظاہر ہونا شروع ہوجاتے ہیں۔ وہ کسی ویب سائٹ کو کھولنے کی کوشش کررہے ہوتے ہیں جبکہ کھل کچھ اور جاتی ہیں۔ چونکہ ان سے چھٹکارا حاصل کرنا مبتدیوں کے لئے اتنا آسان نہیں ہوتا لہٰذا لاعلمی کی وجہ سے انہیں ونڈوز کی ری انسٹالیشن ہی آسان حل نظر آتی ہے۔

کسی کمپیوٹر میں pop-up اشتہارات کی سب سے بڑی وجہ adware کا انسٹال ہوجانا ہے۔ ایڈویئر سافٹ ویئر کی ایسی قسم ہے جو صارف کی نظروں سے اوجھل رہ کر انسٹال ہوجاتے ہیں اور پھر مختلف مواقع پر اشتہارات کی بھرمار کردیتے ہیں۔ خاص طور پر انٹرنیٹ استعمال کرتے ہوئے اشتہارات کی قطاریں لگ جاتی ہیں جنہیں کئی بار نہ تو بند کیا جاسکتا ہے اور اگر بند کر بھی دیا جائے تو اشتہار پر مبنی نئی ونڈو کھل جاتی ہے۔

یہ بات یاد رکھیں کہ ایڈویئر میں بذاتِ خود کسی کمپیوٹر میں داخل ہونے کی صلاحیت نہیں ہوتی۔ یہ صارف کی لاعلمی کا فائدہ اُٹھا کر کمپیوٹر میں انسٹال ہوتے ہیں۔ ان کا آسان حدف تجسس کے ہاتھوں جلدی مجبور ہوجانے والے افراد ہوتے ہیں۔ زیادہ تر کیسز میں یہ کسی دوسرے سافٹ ویئر کے ساتھ نتھی ہوکر آتے ہیں۔ یعنی آپ نے انٹرنیٹ سے کوئی سافٹ ویئر ڈاؤن لوڈ کرکے انسٹال کیا تو ساتھ ہی کوئی ایڈویئر بھی انسٹال ہوجاتا ہے۔

انٹرنیٹ پر سرفنگ کے دوران کئی ویب سائٹس پر ایسے اشتہارات دیکھنے کو ملتے ہیں جن میں کوئی ایسا سافٹ ویئر مفت ڈاؤن لوڈ کرنے کی پیشکش کی گئی ہوتی ہے جو آپ کے کمپیوٹر کی رفتار یا انٹرنیٹ کی رفتار یا کمپیوٹر کے دیگر عام مسئلوں کو چٹکیوں میں ختم کردے گا۔ یہ اشتہارات دل للچا دینے والے دعووں پر مشتمل ہوتے ہیں۔ اسی لئے معصوم لوگ ان کے جھانسے میں آکر انہیں انسٹال کرلیتے ہیں اور یوں خود ہی اپنے کمپیوٹر کو ایڈویئر کا شکار بنا ڈالتے ہیں۔ ماضی میں کچھ مفت سافٹ ویئر جن کی شہرت انتہائی اچھی تھی اور انہیں بنانے والی کمپنیاں بھی معتبر تھیں، کثرت سے استعمال کئے گئے۔ لیکن بعد میں معلوم ہو کہ ان کے مفت سافٹ ویئر میں بھی ایڈویئر شامل تھے۔ اس لئے مشورہ دیا جاتا ہے کہ کبھی بھی کسی اجنبی ویب سائٹ سے مفت سافٹ ویئر ڈاؤن لوڈ کرکے انسٹال نہ کریں۔

ایڈویئر اور اسپائی ویئر اتنے عام ہیں کہ مائیکروسافٹ نے ونڈوز وستا کے بعد سے ونڈوز ڈیفنڈر کو ونڈوز کا حصہ ہی بنا دیا ہے۔ یہ سافٹ ویئر ونڈوز کو ایڈویئر اور اسپائی ویئر سے

محفوظ رکھتا ہے۔

اگر بدقسمتی سے آپ کا کمپیوٹر کسی ایڈ ویئر کا شکار ہوچکا ہے تو ونڈوز ری انسٹال کرنے کی ضرورت نہیں۔ ایڈ ویئر سے نجات دلانے کے لئے کئی سافٹ ویئر دستیاب ہیں۔ اب تقریباً تمام ہی اینٹی وائرسز میں اینٹی ایڈ ویئر انجن بھی شامل ہوتا ہے۔ اگر آپ کے کمپیوٹر میں کوئی اینٹی وائرس انسٹال ہے تو اسے اپ ڈیٹ کرکے کمپیوٹر کو اسکین کیجئے تاکہ اگر وہ ایڈ ویئر کو تلاش کرکے چھٹکارا دلاسکتا ہے تو اُسے موقع دیا جائے۔

کچھ سافٹ ویئر جنہیں اینٹی ایڈ ویئر کہا جاتا ہے، خاص طور پر اسی مقصد کے لئے بھی دستیاب ہیں۔ ان میں سے ایک مفت اور قابل بھروسا سافٹ ویئر مال ویئر بائٹس اینٹی مال ویئر (Malware Bytes Anti-Malware) ہے۔ اگر آپ کا اینٹی وائرس ناکام ہوچکا ہے تو اسے آزمانے میں کوئی حرج نہیں۔ اسے درج ذیل ربط سے ڈاؤن لوڈ کیا جاسکتا ہے:

www.malwarebytes.org/mwb-download

یاد رہے کہ اگر آپ نے پہلے سے کوئی اینٹی وائرس انسٹال کررکھا ہے تو مال ویئر بائٹس اینٹی مال ویئر کو انسٹال کرنے سے پہلے اسے غیر فعال (ڈِس ایبل) کردیں۔ جس طرح ایک میان میں دو تلواریں نہیں آسکتیں، اسی طرح ایک کمپیوٹر میں دو چلتے ہوئے اینٹی مال ویئر بھی نہیں ہونے چاہئیں۔

مال ویئر بائٹس اینٹی مال ویئر انسٹال کرنے کے بعد کمپیوٹر کی مکمل اسکیننگ کیجئے۔ یہ کچھ وقت لے گا لیکن آپ کے کمپیوٹر کو ہر قسم کے خراب سافٹ ویئر سے پاک کردے گا۔

⑤ ویب سائٹ کی ہیئت عجیب نظر آرہی ہے

یہ بھی ایک عام مسئلہ ہے اور گزشتہ مسئلے سے ملا جلا ہے۔ آپ نے فائر فاکس میں google.com لکھ کر انٹر کیا۔ لیکن یہ کیا! گوگل کی ویب سائٹ تو معمول سے مختلف نظر آرہی ہے۔ گوگل کا ہوم پیج جو اشتہارات سے پاک ہوتا ہے، اب اشتہارات سے اٹا پڑا ہے۔ یہ براؤزر ہائی جیکنگ کی وجہ سے ہے۔ کچھ مال ویئر عام استعمال ہونے والے ویب براؤزر جیسے انٹرنیٹ ایکسپلورر، فائر فاکس اور کروم میں ایکسٹینشن کی سہولت کا فائدہ اٹھا کر ان سے جڑ جاتے ہیں۔ کسی براؤزر میں ایکسٹینشن یا ایڈ اونز کی سہولت اس لئے فراہم کی جاتی ہے کہ پروگرامرز ان کے ذریعے ویب براؤزر کی صلاحیت میں اضافہ کرسکیں۔ مثلاً جب آپ FoxIt پی ڈی ایف ریڈر انسٹال کرتے ہیں تو وہ براؤزر ایکسٹینشن انسٹال کرکے براؤزر کو اس قابل بنا دیتا ہے کہ پی ڈی ایف فائلیں براہ راست اس میں دیکھی جاسکتی ہیں۔ لیکن بدنیت لوگ اس سہولت کا بھی غلط فائدہ اٹھاتے ہیں۔ جعلی سافٹ ویئر (جو دعویٰ کچھ کرتے ہیں لیکن ہوتے کچھ ہیں) جب کمپیوٹر میں انسٹال کئے جاتے ہیں تو وہ ویب براؤزر میں مختلف ایکسٹینشن یا ایڈ اونز (ٹول بارز بھی ایکسٹینشن کی ہی ایک قسم ہے) بھی انسٹال کردیتے ہیں۔ ایکسٹینشن کے پاس صارف کو نظر آنے والے ویب پیج میں تبدیلی کرنے کی صلاحیت ہوتی ہے۔ یعنی یہ ایکسٹینشن چاہیں تو براؤزر میں نظر آنے والے ویب پیج کا حلیہ بالکل تبدیل کرسکتے ہیں۔

یہ نقصان دہ براؤزر ایکسٹینشن اتنے عام ہیں کہ اب اچھے اینٹی وائرس سسٹم میں ان کے خلاف مدافعت کا انتظام بھی موجود ہوتا ہے۔ تاہم اگر آپ اس کا شکار ہوچکے ہیں تو پھر آپ کو خود براؤزر کو صاف کرنا ہوگا۔

ہر براؤزر اگر ایکسٹینشن کو انسٹال کرنے کی سہولت دیتا ہے تو انہیں غیر فعال یا ڈِس ایبل کرنے کی سہولت بھی اس میں موجود ہوتی ہے۔ انٹرنیٹ ایکسپلورر میں ایکسٹینشن اور ایڈ اونز کو غیر فعال کرنے کے لئے Tools مینو پر کلک کریں۔ اگر یہ آپ کو

نظر نہ آ رہا ہو تو کی بورڈ سے ALT کا بٹن دبائیں۔ ٹولز مینو میں سے Manage Add-ons کے تحت موجود Enable or Disable Add-ons پر کلک کیجئے۔ کھلنے والی ونڈو میں سے تمام نامعلوم اور غیر ضروری ایڈ اونز کو منتخب (select) کر کے غیر فعال کر دیں۔

فائر فاکس میں یہ کام کرنے کے لئے ایڈریس بار میں about:addons لکھ کر اینٹر کریں اور کھولنے والے پیج میں سے بائیں جانب موجود Extensions پر کلک کر کے تمام غیر ضروری ایکسٹینشن ڈِس ایبل کر دیں۔

گوگل کروم میں فعال اور غیر فعال ایکسٹینشن کی فہرست دیکھنے کے لئے ایڈریس بار میں chrome://plugins لکھ کر اینٹر کریں۔ کھلنے والے پیج میں تمام ایکسٹینشن کی فہرست ہوگی جس میں سے آپ جسے مناسب سمجھیں disable کر دیں۔

⑥ سکیورٹی سرٹیفکیٹ کے ساتھ مسئلہ ہے

کئی بار آپ کسی ویب سائٹ کو کھولنے کے لئے اس کا ایڈریس ٹائپ کر کے اینٹر کرتے ہیں تو ویب سائٹ کھلنے کے بجائے ایک ایرر ظاہر ہوتا ہے کہ اس ویب سائٹ کے سکیورٹی سرٹیفکیٹ کے ساتھ کوئی مسئلہ ہے۔ یہ ایرر ہر براؤزر میں ظاہر ہوتا ہے۔ لیکن بظاہر سنگین لگنے والا یہ مسئلہ دراصل ایک اطلاع ہے۔ اس مسئلے کو سمجھنے کے لئے پہلے آپ کو سکیورٹی سرٹیفکیٹ کو سمجھنا ہوگا۔

ویب سائٹ اور آپ کے کمپیوٹر کے درمیان ڈیٹا کے تبادلے کو محفوظ بنانے کے لئے https پروٹوکول کا استعمال کیا جاتا ہے۔ اس پروٹوکول کے استعمال سے آپ کے کمپیوٹر سے ویب سائٹ اور ویب سائٹ سے کمپیوٹر تک آنے والا ڈیٹا اِنکرپٹ (encrypt) کر دیا جاتا ہے۔

انکرپٹ کرنے کے لئے ویب سائٹ کا سرور ویب براؤزر کو ایک خاص فائل فراہم کرتا ہے جسے سرٹیفکیٹ کہا جاتا ہے۔ ہر ویب سائٹ کے لئے مخصوص سرٹیفکیٹ ہوتا ہے۔ آپ کہہ سکتے ہیں کہ یہ سرٹیفکیٹ ویب سائٹ کی پہچان ہوتی ہے۔ اس سرٹیفکیٹ میں ایک کلید (Key) جسے Public Key کہا جاتا ہے، موجود ہوتی ہے۔ اسی کلید کے ذریعے ویب براؤزر ویب سائٹ کو ڈیٹا بھیجنے سے پہلے اِنکرپٹ کرتا ہے۔ ویب سائٹ کے سرور کے پاس اپنی ایک خفیہ کلید ہوتی ہے جسے پرائیوٹ کی کہا جاتا ہے۔ پرائیوٹ کی صرف سرور کے پاس ہونی چاہئے جبکہ پبلک کی کو ہر براؤوزر کے ساتھ شیئر کیا جاسکتا ہے۔ پبلک کی کے ذریعے انکرپٹ کیا گیا ڈیٹا صرف پرائیوٹ کی کے ذریعے ہی ڈی کوڈ یا ڈی کرپٹ کیا جاسکتا ہے۔ یعنی سرٹیفکیٹ اس سارے عمل میں انتہائی اہم کردار ادا کرتا ہے اور اس کا سو فی صد درست ہونا ضروری ہے۔

سرٹیفکیٹ کی درستگی جانچنے کے لئے آپ کا ویب براؤزر سرٹیفکیٹ جاری کرنے والے ادارے کے ڈیٹا بیس سے رابطہ کرتا ہے اور سرٹیفکیٹ کی تصدیق کرتا ہے کہ آیا وہ درست ہے کہ نہیں۔ اگر کوئی سرٹیفکیٹ abc.com کے لئے جاری کیا گیا ہے تو اسے xyz.com پر استعمال نہیں کیا جاسکتا۔ ایسی صورت میں براؤزر خرابی کی نشاندہی کرے گا۔ یہ بھی یاد رہے کہ ہر سرٹیفکیٹ کو کچھ معیاد کے لئے ہی جاری کیا جاتا ہے۔ یہ معیاد ایک سال سے کئی سال تک ہو سکتی ہے۔ تاہم عام طور پر یہ ایک سے پانچ سالوں کے لئے جاری کئے جاتے ہیں۔ معیاد پوری ہو جانے کے بعد انہیں دوبارہ جاری کروانا پڑتا ہے۔

چونکہ سرٹیفکیٹ کی درستگی سو فی صد ہونا ضروری ہے اس لئے ویب براؤزر سرٹیفکیٹ کی تاریخ اجراء اور تاریخ تنسیخ بھی چیک کرتا ہے۔ اگر آپ کے کمپیوٹر کی گھڑی میں تاریخ و وقت درست نہیں ہو تو ویب براؤزر سرٹیفکیٹ کو جعلی تصور کر لیتا ہے۔ وجہ سادہ سی ہے، ویب براؤزر کو بذات خود تاریخ اور وقت کا نہیں پتا ہوتا اور وہ آپ کے کمپیوٹر کی گھڑی پر ہی انحصار کرتا ہے۔ یعنی مسئلہ جس کی تفصیل بیان کرنے میں ہم نے پورا ایک صفحہ کالا کر دیا ہے، کو حل کرنے کے لئے آپ کو صرف کمپیوٹر کی گھڑی میں وقت درست کرنا ہوگا!

بعض اوقات ویب سائٹ کا سکیورٹی سرٹیفکیٹ حقیقتاً اپنی معیاد پوری کر چکا ہوتا ہے اور ویب سائٹ کے مالک اس کے سرٹیفکیٹ کی تجدید نہیں کرواتے۔ لہٰذا اگر آپ کے کمپیوٹر کے گھڑی میں تاریخ اور وقت بالکل ٹھیک ہے تو پھر مسئلہ ویب سائٹ کے سرٹیفکیٹ کے ساتھ ہی ہے اور اسے حل کرنا آپ کے اختیار میں نہیں۔

⑦ پرنٹر کام نہیں کر رہا

یہ بھی ایک عام مسئلہ ہے جس کی کئی وجوہ ہوسکتی ہیں۔ سب سے پہلے تو پرنٹر کا ڈرائیور چیک کرلینا چاہئے کہ آیا وہ انسٹال بھی ہے کہ نہیں اور کیا وہ تار جس سے پرنٹر کمپیوٹر سے جوڑا گیا ہے، ٹھیک ہے کہ نہیں۔ اگر یہ دونوں ہی درست ہیں تو دوسری وجہ پرنٹر کا آف لائن ہونا ہوسکتی ہے۔ جب آپ پرنٹر کو چلانے کے بعد اس کی پاور آف کردیتے ہیں تو پرنٹر آف لائن موڈ میں چلا جاتا ہے۔

آف لائن موڈ میں آپ جن ڈاکیومنٹس کو پرنٹ کرتے ہیں، کمپیوٹر انہیں اپنے پاس محفوظ کرتا جاتا ہے اور جیسے ہی پرنٹر دوبارہ آن لائن آتا ہے (اُسے آن کیا جاتا ہے) ڈاکیومنٹس پرنٹ ہونا شروع ہوجاتے ہیں۔ یہ دیکھنے کے لئے کہ آیا پرنٹر آف لائن ہے یا آن لائن، اسٹارٹ مینو میں سے کنٹرول پینل اور پھر Devices and Printer پر کلک کریں۔ یہاں سے اپنے پرنٹر کے آئی کن پر ڈبل کلک کریں جس سے print queue ونڈو کھل جائے گی۔ اس ونڈو میں وہ تمام ڈاکیومنٹس دیکھے جاسکتے ہیں جو پرنٹ ہونے کے لئے اپنی باری کے انتظار میں ہیں۔ اس ونڈو میں Printer کے مینو پر کلک کریں۔ اگر اس مینو میں Use Printer Offline کے آپشن کے ساتھ چیک مارک (check mark) موجود ہے تو آپ کا پرنٹر آف لائن موڈ میں ہے۔ اگر پرنٹر آف ہے تو اسے آن کرنے سے یہ چیک مارک خود ہی ہٹ جائے گا۔ لیکن اگر ایسا نہیں ہوتا تو آپ اس پر کلک کرکے پرنٹر کو دوبارہ آن لائن کرسکتے ہیں۔

پرنٹر کے آف لائن ہونے کی ایک نشانی یہ بھی ہے کہ print queue ونڈو کے ٹائٹل میں Use Printer Offline لکھا ہوتا ہے۔

پرنٹر کے پرنٹ نہ دینے کی ایک وجہ Spooler سروس کی خرابی بھی ہوسکتی ہے۔ اگر پرنٹر کا ڈرائیور بھی انسٹال ہے اور وہ آف لائن بھی نہیں تو رن ڈائیلاگ باکس میں services.msc لکھ کر اینٹر کریں اور Print Spooler سروس پر رائٹ کلک کرکے restart کردیں۔

بعض اوقات صرف پرنٹر کے تار کو کمپیوٹر سے الگ کرکے دوبارہ لگانے سے بھی مسئلہ حل ہوجاتا ہے۔

⑧ وائی فائی بار بار ڈس کنکٹ ہورہا ہے

چونکہ وائی فائی ڈیوائسز اب بہت عام ہیں، اس لئے وائی فائی کنکشن کا بار بار ڈس کنکٹ ہوجانا بھی ایک عام مسئلہ ہے۔ اس مسئلے کی دو اہم وجوہ ہیں۔ اگر وائی فائی ہاٹ اسپاٹ آپ سے خاصے فاصلے پر ہے اور اس کے سگنلز کمزور ہیں تو وائی فائی کنکشن بار بار منقطع ہوتا رہے گا۔ دوسری وجہ ڈیوائس یا ہاٹ اسپاٹ کی غلط کنفگریشن ہے۔ اس مسئلے سے آپ وائی فائی ڈیوائس یا روٹر پر موجود Restore to default یا reset کا آپشن استعمال کرکے نجات حاصل کرسکتے ہیں۔

ایک چیز اور ذہن میں رکھیں کہ ہر ہاٹ اسپاٹ یا وائی فائی روٹر سے ڈیوائسز کی ایک محدود تعداد ہی کنکٹ ہوسکتی ہے۔ روٹر فروخت کرنے والی کمپنیاں اس تعداد کے بارے میں واضح ہدایات ڈبے پر لکھتی ہیں۔ اگر روٹر پر ڈیوائسز کا رش بڑھ جائے تو بھی وائی فائی کنکشن کے بار بار منقطع ہونے کا مسئلہ پیدا ہوتا ہے۔

یہ بھی ممکن ہے کہ آپ نے ایک زیادہ سے ہاٹ اسپاٹ کے ساتھ کنکشن بنائے اور محفوظ کررکھے ہوں۔ اس صورت میں ایک ہاٹ اسپاٹ کے کمزور سگنلز کی صورت میں یہ وائی فائی ڈیوائس دوسرے ہاٹ اسپاٹ سے کنکٹ ہونے کی کوشش کرتی ہے۔ لہٰذا وہ ہاٹ اسپاٹ جن کے سگنلز کمزور ہوں، انہیں Forget یا ڈیلیٹ کردیا کریں۔

ایسا بھی دیکھا گیا کہ وائی فائی ڈیوائس اور روٹر بنانے والی کمپنیوں کی ہی جانب سے کوئی خرابی پیدا ہوتی ہے جسے دور کرنے کے لئے یہ نئے فرم ویئر اور ڈرائیورز ڈاؤن لوڈنگ کے لئے فراہم کرتے ہیں۔ اس لئے جب بھی وائی فائی کے ساتھ کوئی مسئلہ درپیش ہو، اس بات کی تصدیق کرلیں کہ آپ کے پاس تازہ ترین ڈیوائس ڈرائیور اور فرم ویئر انسٹال ہے۔

ڈیوائس ڈرائیورز اور فرم ویئر کے بارے میں معلومات ڈیوائس بنانے والے ادارے کی ویب سائٹ سے باآسانی حاصل کی جاسکتی ہے۔ جبکہ کئی ڈیوائس ڈرائیور تو صرف ونڈوز کو اپ ڈیٹ کرنے سے بھی اپ ڈیٹ ہوجاتے ہیں۔

(جاری ہے)

سب دوستوں سے چیٹ کریں اور ایس ایم ایس بھیجیں ایک ہی پلیٹ فارم سے

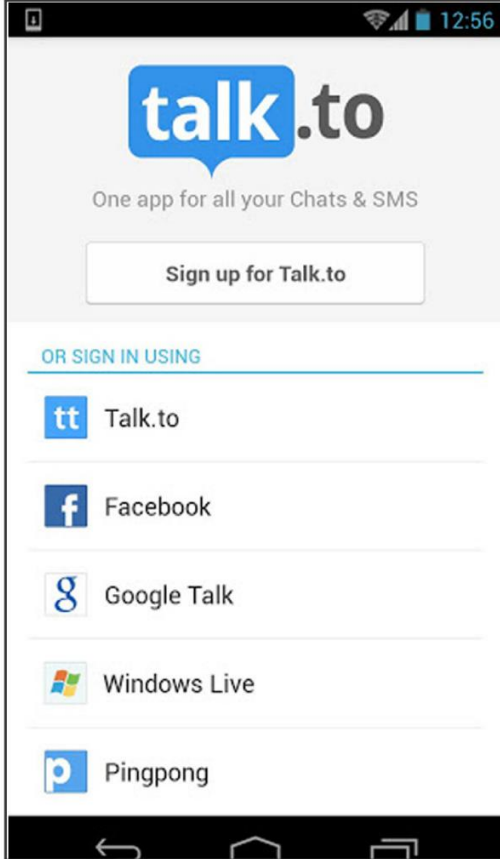
ہم دن بھر انٹرنیٹ استعمال کرتے ہیں۔ انٹرنیٹ استعمال کریں اور کسی سے چیٹ نہ کریں یہ ممکن نہیں۔ دوسروں سے رابطے کے لیے چیٹ ایک بہترین طریقہ ہے۔ اس لیے کبھی چیٹ کے لیے جی میل استعمال کیا جاتا ہے تو کبھی ونڈوز لائیو، اس کے علاوہ چیٹ کے لیے فیس بک بھی کثرت سے استعمال ہوتا ہے۔ کچھ دوست جی میل پر آن لائن ہوتے تو کچھ لائیو پر، اور دوستوں کی ایک بڑی تعداد فیس بک پر بھی آن لائن ہوتی ہے۔ اس طرح ہمیں ہر جگہ آن لائن رہنا پڑتا ہے تاکہ سب سے رابطے میں رہیں۔ اگر تمام دوستوں سے ایک جگہ چیٹ ہوجائے تو یہ کام کس قدر سہل ہوجائے؟ اگرچہ اس کام کے لیے کئی ایپلی کیشنز دستیاب ہیں لیکن آپ کا تعارف ایک نئی اور دلچسپ ایپ سے کراتے ہیں۔ اس ایپلی کیشن کا نام ہے ''ٹالک ڈاٹ ٹو'' (Talk.to)۔

یہ ٹالک ایپلی کیشن ڈیسک ٹاپ کے لیے کروم براؤزر میں دستیاب ہے اس کے علاوہ یہ آئی او ایس، اینڈرائیڈ اور ونڈوز فون کے لیے بھی دستیاب ہے۔ ڈیسک ٹاپ پر اسے استعمال کرنے کے لیے ضروری ہے کہ پہلے اسے فون پر انسٹال کیا جائے۔ اس ایپلی کیشن میں آپ اپنا جی میل، لائیو اور فیس بک اکاؤنٹ کنفیگر کر کے تمام دوستوں کے ساتھ ایک ہی پلیٹ فارم سے چیٹ کرسکتے ہیں۔

فیس بک اکاؤنٹ اس میں کنفیگر کرتے ہوئے یہ ایپلی کیشن آپ کی وال پر پوسٹس کرنے کی اجازت مانگتی ہے۔ اگر آپ چاہیں تو اسے یہ اجازت دے سکتے ہیں اور اگر پسند نہ کریں تو اسے منع کرسکتے ہیں۔

کی گئی تمام چیٹس اصل ویب سائٹ کی چیٹ ہسٹری میں ہی محفوظ رہتی ہیں۔ اسی طرح پرانی چیٹ ہسٹری کو لے کر چیٹ کو آگے بھی بڑھایا جاسکتا ہے۔ گروپ چیٹ کی سہولت اس ایپلی کیشن کا ایک اور بہترین فیچر ہے۔

اس ایپلی کیشن کی خاص بات یہ ہے کہ یہ 200 ایس ایم ایس بھی مفت بھیجنے کی سہولت دیتی ہے۔ اس کے علاوہ ہر اتوار کے دن اضافی 5 ایس ایم ایس بھی مفت آپ کے اکاؤنٹ میں شامل کردیے جاتے ہیں۔

http://talk.to

جو کال ریسیو نہ کرے اس کا فون لاک کریں (اینڈرائیڈ)

آج کل جو حالات ہیں ماں باپ اپنے بچوں کے بارے میں بہت فکر مند رہتے ہیں۔ جب کہ نوجوانوں کو ماں باپ کی فکر و پریشانی کا کوئی اندازہ نہیں ہوتا۔ حتیٰ کہ گھر سے آنے والی کالز تک اٹینڈ نہیں کرتے۔ اس مسئلے کا بڑا آسان لیکن ایک سخت حل موجود ہے اور اس حل یعنی اپلی کیشن کا نام ہے ''اگنور نو مور'' (Ignore No More)۔ یعنی اس اپلی کیشن کے ہوتے ہوئے مزید نظر انداز کرنا ممکن نہیں۔

اپلی کیشن کے فیچرز کو استعمال کرنے کے لیے دونوں ڈیوائسز پر اس کا انسٹال ہونا ضروری ہے۔ پہلے اپنے فون پر اسے انسٹال کر کے اکاؤنٹ بنانا پڑے گا۔ یہ اکاؤنٹ بطور Parent بنے گا۔ اس کے بعد جس فون کو کنٹرول کرنا ہو اس پر یہ اپلی کیشن انسٹال کر کے اپنا اکاؤنٹ لاگ اِن کریں اور اس فون کو بطور Child کنفیگر کر لیں۔ ایک اکاؤنٹ کے اندر ایک سے زائد ڈیوائسز کو بطور چائلڈ ڈیوائس ایڈ کیا جاسکتا ہے۔

اپلی کیشن کا استعمال بہت ہی سادہ ہے کہ جب آپ کی بار بار کی گئی فون کالز اور پیغامات کا جواب موصول نہ ہو تو اپنے اکاؤنٹ سے لاگ اِن ہو کر اُن کی ڈیوائس کو بلاک کر دیں۔ بلاک ہونے کے بعد فون کسی کام کا نہیں رہے گا۔ فون کا بلاک ہونا آج کل ایک منی ہارٹ اٹیک کے برابر ہے اس لیے امید ہے کہ فوراً ہی وہاں سے کال آجائے گی اور تسلی کے بعد آپ فون اَن بلاک کر سکتے ہیں۔

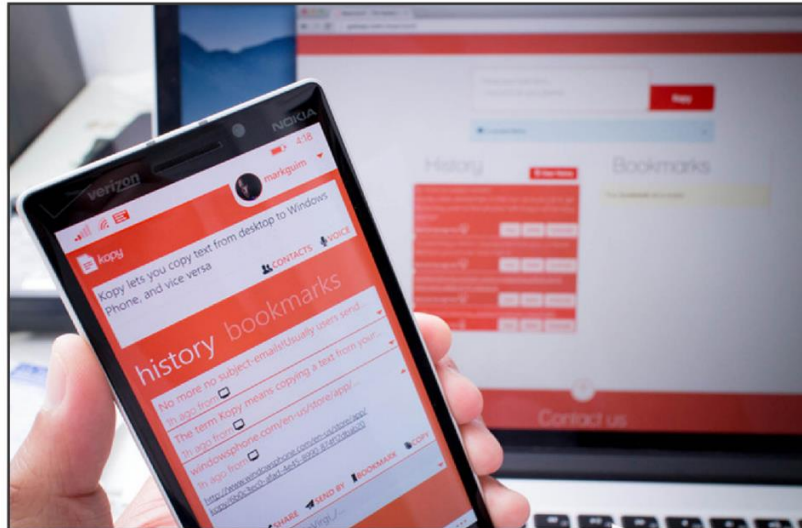
ignorenomoreapp.com

پی سی سے فون پر معلومات شیئر کریں (ونڈوز فون)

اکثر کوئی مواد کمپیوٹر پر پڑھتے ہوئے اسے فون پر محفوظ کرنے کی ضرورت ہوتی ہے۔ اس کام کے لیے ''کوپی'' نامی اپلی کیشن ونڈوز فون کے لیے دستیاب ہے۔ اس اپلی کیشن کا کام انتہائی سادہ ہے۔ سب سے پہلے فون پر اس کی انسٹالیشن ضروری ہے اور ایک عدد اکاؤنٹ بنانا پڑتا ہے۔ اب کمپیوٹر سے کوئی بھی ٹیکسٹ فون پر بھیجنے کے لیے کوپی کی ویب سائٹ پر جائیں اور وہاں بھی اپنے اکاؤنٹ سے لاگ اِن ہو جائیں۔

لاگ اِن ہونے کے بعد یہاں دی گئی ٹیکسٹ کی فیلڈ میں ٹیکسٹ پیسٹ کر کے یا لکھ کر انٹر پریس کر دیں۔ وہ ٹیکسٹ آپ کو فوراً ہی فون پر موصول ہو جائے گا۔

اسی طرح موبائل فون سے ٹیکسٹ پی سی پر بھی بھیجا جا سکتا ہے۔ اس کام کے لیے کوپی اپلی کیشن میں ٹیکسٹ پیسٹ کر کے بھیجیں اور اس کی ویب سائٹ پر جائیں، وہاں یہ ٹیکسٹ آپ کا منتظر ہوگا۔ ای میل ایڈریس، ایس ایم ایس یا فون نمبرز وغیرہ کو کاپی کرنے کے لیے یہ ایک بہترین حل ہے۔

http://gokopy.com

فون سے فائلیں کاپی کریں بذریعہ وائی فائی (اینڈرائیڈ)

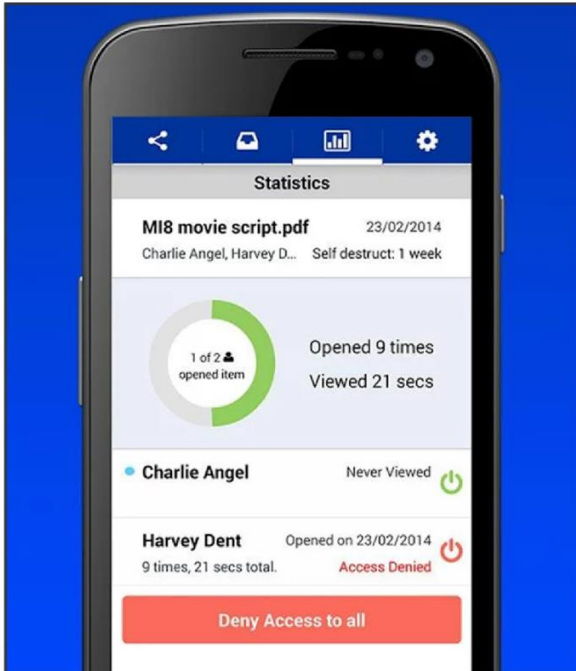
جب بھی فون سے کچھ فائلز کاپی کرنے کی ضرورت ہوتی ہے ہم یو ایس بی کیبل تلاش کرتے ہیں۔ تاکہ فون کو پی سی سے کنیکٹ کر کے فائلز کاپی کی جاسکیں۔ جب فون اور کمپیوٹر ایک ہی وائی فائی کنکشن استعمال کرتے ہوئے ایک ہی نیٹ ورک پر ہیں تو کیوں نا فون سے فائلز بذریعہ ایف ٹی پی کاپی کر لی جائیں؟

اس کام کے لیے آپ کو اپنے اینڈرائیڈ فون پر ایک اپلی کیشن WiFi FTP انسٹال کرنی ہوگی۔ یہ اپلی کیشن ایک چھوٹا سا ایف ٹی پی سرور چلا دیتی ہے جسے نیٹ ورک پر رہتے ہوئے استعمال کیا جاسکتا ہے۔ فون ڈیٹا کی حفاظت کے لیے اس ایف ٹی پی رابطے کے لیے یوزرنیم اور پاس ورڈ استعمال کیا جاتا ہے جو کہ فون پر اپلی کیشن انسٹال کر کے بنایا جاتا ہے۔

اپلی کیشن کی سیٹنگز کرتے ہوئے یوزرنیم پاس ورڈ کے بعد پورٹ نمبر منتخب کرنا ہوتا ہے دیگر ایف ٹی پی کنکشنز کی طرح یہاں پورٹ 21 مت منتخب کریں۔ اس کی جگہ آپ 2121 یا 2222 بطور پورٹ ٹائپ کر سکتے ہیں۔ اس کے علاوہ یوزرنیم اور پاس ورڈ کی فیلڈ اگر خالی چھوڑ دیں تو فون کو بنا لاگ اِن تفصیلات کے بھی کنیکٹ کیا جاسکے گا۔

یہ سیٹنگز کرتے ہی اپلی کیشن آپ کو ایف ٹی پی ایڈریس فراہم کر دے گی، جسے براؤزر یا ایکسپلورر میں ٹائپ کرنے سے فون کا سارا ڈیٹا سامنے ہوگا۔

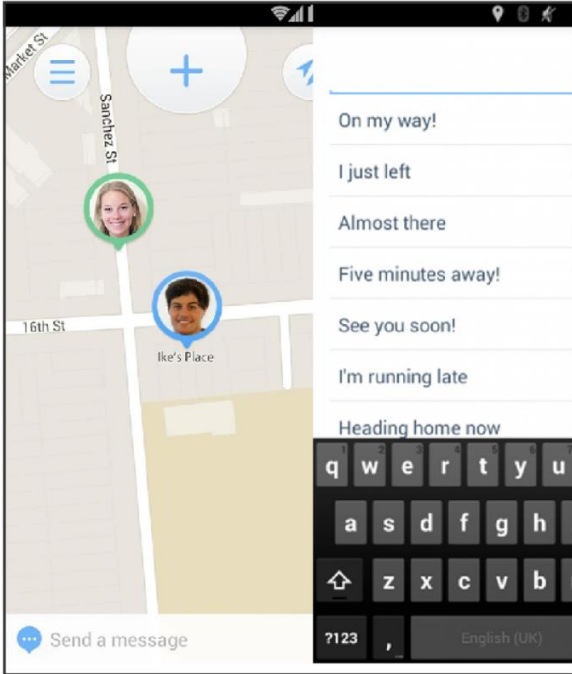
http://bit.ly/wifi-ftp

ذاتی فائلیں حفاظت سے شیئر کریں (آئی او ایس و اینڈرائیڈ)

فائلز شیئر کرنا ہمارا روزمرہ کا کام ہے۔ لیکن ایک دفعہ فائل کسی کو بھیج دینے کے بعد آپ کو اس پر کوئی اختیار نہیں رہتا۔ فائل موصول کرنے والا اسے کسی کو بھی آگے بھیج سکتا ہے۔ فائل شیئرنگ کے لیے ''ڈگی فائی'' (Digify) اپلی کیشن موجود ہے۔ یہ اپلی کیشن ڈراپ باکس کے ساتھ کام کرتی ہے۔ اس کے ذریعے شیئر کی گئی فائل کو موصول کرنے والا فاورڈ نہیں کر سکتا۔ اس کے علاوہ نہ ڈاؤن لوڈ کیا جاسکتا ہے اور نہ ہی اس کا اسکرین شاٹ بنایا جاسکے گا۔

فائلوں کو آپ محدود دورانیے کے لیے بھی شیئر کر سکتے ہیں۔ مثلاً آپ چاہیں کہ فائل موصول ہونے کے اتنے منٹس بعد یا اتنے دن بعد خود بخود ختم ہو جائے تو یہ بھی ممکن ہے۔ اس کے علاوہ یہ اپلی کیشن آپ کو یہ بھی بتاتی ہے کہ فائل کو کتنی بار اور کتنی دیر تک دیکھا گیا۔

اس اپلی کیشن کو استعمال کرنے کے لیے آپ کے پاس ڈراپ باکس اکاؤنٹ ہونا چاہیے۔ شیئر کی گئی فائل کا لنک بذریعہ ای میل بھیجا جاتا ہے لیکن موصول کنندہ کو فائل دیکھنے کے لیے یہ اپلی کیشن انسٹال کرنی پڑتی ہے۔

www.digify.com

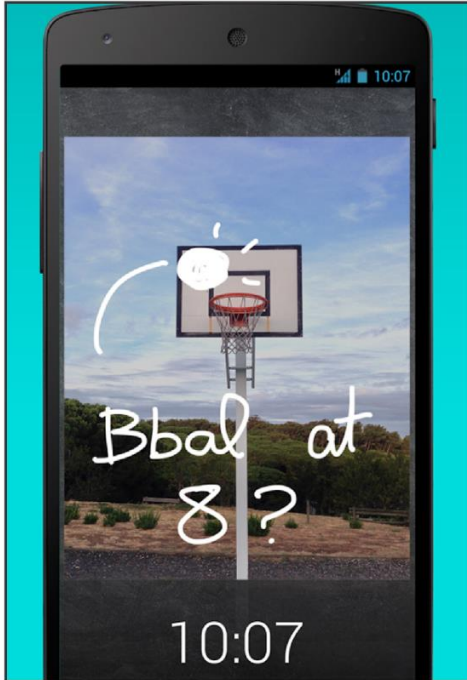
ایک دوسرے کے موجودہ مقام سے آگاہ رہیں (آئی او ایس وانیڈرائیڈ)

موبائل فون کے عام ہونے سے سب سے بڑا فائدہ یہی ہوا کہ اب سب ایک دوسرے کے رابطے میں ہیں۔ کسی سے بھی رابطہ کر کے جانا جا سکتا ہے کہ وہ کہاں ہے۔ اگر آپ اپنے کسی دوست یا فیملی ممبر کی لوکیشن یعنی موجودہ مقام سے باخبر رہنا چاہتے ہیں تو "جِنک" ایپلی کیشن انسٹال کرنی ہوگی۔

Jink کی انسٹالیشن کے بعد جس سے رابطے میں رہنا ہو اسے پیغام بھیجیں، جس میں اس ایپلی کیشن کو ڈاؤن لوڈ کرنے کا ربط موجود ہوگا۔ دوسری طرف اس کی انسٹالیشن کے بعد اب دونوں ایک دوسرے کا موجودہ مقام ایک نقشے کے ذریعے جان سکتے ہیں۔

اس کے علاوہ اس میں چند پیغامات بھی پہلے سے موجود ہوتے ہیں۔ یعنی بنا ٹائپ کیے پیغام بھیجا جا سکتا ہے کہ میں اتنے منٹس میں پہنچ رہا ہوں، یا کہ لیٹ ہوں یا کہ میں مقررہ مقام پر پہنچ کر انتظار کر رہا ہوں۔

اپنے فیملی ممبرز کی حفاظت کے بارے میں فکرمند لوگ اس ایپلی کیشن کے استعمال سے مطمئن رہ سکتے ہیں۔

www.jinkapp.com

"لاک لاک" ایک منفرد اسکرین لاک (اینڈرائیڈ)

LokLok ایپلی کیشن ابھی مکمل ورژن میں دستیاب نہیں لیکن اس کا بے ٹا ورژن استعمال کے لیے موجود ہے۔ اس ایپلی کیشن کا انداز بالکل اچھوتا ہے۔ اسے ایک میسنجر ایپلی کیشن کی طرح آپ اور آپ کے دوستوں کے پاس انسٹال ہونا چاہیے تاکہ سب رابطے میں رہ سکیں۔ لیکن یہ رابطہ صرف لاک اسکرین کے ذریعے رہتا ہے۔ جتنے لوگ رابطے میں ہوں گے سب کی لاک اسکرین ایک جیسی دکھائی دے گی۔

دراصل اس میں اسکرین کو ایک وائٹ بورڈ سے بدل دیا جاتا ہے۔ جس پر آپ کچھ بھی لکھ سکتے ہیں یا کوئی ڈرائنگ بنا سکتے ہیں۔ یہ اسکرین رابطے میں موجود تمام لوگوں کے پاس موجود فون کی اسکرین سے sync رہتی ہے۔ اس طرح جو بھی اسکرین پر کوئی میسیج دے گا فوراً سب کی اسکرین پر وہی دکھائی دے گا۔

اسے استعمال کرنے کے لیے فون کو اَن لاک کرنے کی بھی ضرورت نہیں پڑتی۔ اگر آپ کسی کے لیے پیغام چھوڑنا چاہتے ہیں تو بس اپنا فون اٹھائیں اور لاک اسکرین پر ہی کچھ لکھ دیں۔ آپ کا پیغام فوراً سب تک پہنچ جائے گا۔ کوئی بھی پروگرام یا ملاقات طے کرنے کے لیے یہ ایپلی کیشن ایک بہترین ذریعہ ہے۔

http://loklok.co

گلاس ویئر-نیٹ ورک مونیٹر

انٹرنیٹ کی سست رفتاری کی شکایت کرنے والے دوستوں کو اکثر پتا ہی نہیں ہوتا کہ ان کا انٹرنیٹ تو ٹھیک کام کررہا ہے لیکن ان کے کمپیوٹر میں چلتا کوئی پروگرام ان کے انٹرنیٹ کی ساری بینڈ وڈتھ ہضم کررہا ہوتا ہے۔ جس کا نتیجہ یہ نکلتا ہے کہ ویب براؤزنگ اور دیگر انٹرنیٹ پر ہونے والے کام سست رفتار ہوجاتے ہیں۔ اگرچہ ونڈوز وستا اور اس کے بعد کے تمام ورژنز میں مائیکروسافٹ نے ریسورس مونیٹر نامی ٹول فراہم کررکھا ہے جس کے ذریعے صارف دیکھ سکتا ہے کہ اس کا کمپیوٹر انٹرنیٹ یا نیٹ ورک پر کیا کررہا ہے۔ تاہم اس یوٹیلیٹی کے فوائد محدود ہیں۔

گلاس وائر (GlassWire) وہ مفت سافٹ ویئر ہے جو کہ انٹرنیٹ اور نیٹ ورک پر ہونے والی ہر قسم کی ایکٹیویٹی کی تفصیل فراہم کرتا ہے اور ساتھ ہی وائرسز یا مال ویئر کی جانب سے انٹرنیٹ پر ہونے والی حرکات پر بھی نظر رکھتا ہے۔

https://www.glasswire.com/

ایک اور ڈیٹا ریکوری سافٹ ویئر

غلطی سے فائلیں ڈیلیٹ کردینا وہ کام ہے جو کبھی نہ کبھی آپ سے سرزد ہوہی جاتا ہے۔ ڈیلیٹ کی گئی فائلوں کو واپس بحال کرنے کے لئے کئی مفت سافٹ ویئر دستیاب ہیں۔ کمپیوٹنگ کے فروری 2014ء کے شمارے میں ڈیٹا ریکوری کے حوالے سے ایک مفصل مضمون بھی شائع کیا گیا تھا۔ Abyssal Recovery بھی ایک ایسا ہی سافٹ ویئر ہے جو FAT اور NTFS فائل سسٹم سے ڈیلیٹ کیا گیا ڈیٹا واپس بحال کرسکتا ہے۔

یہ صرف ہارڈ ڈسک ہی نہیں بلکہ میموری کارڈ اور فلیش ڈرائیو سے بھی ڈیٹا ریکور کرسکتا ہے۔ دیگر ڈیٹا ریکوری سافٹ ویئر کی طرح اس کے استعمال کے لئے بھی صلاح دی جاتی ہے کہ یا تو ڈیٹا ریکوری سافٹ ویئر کو پہلے سے انسٹال کرکے رکھیں یا پھر کسی دوسری ڈرائیو کو کمپیوٹر کے ساتھ جوڑ کر اس میں انسٹال کریں۔ جس ڈرائیو سے ڈیٹا ڈیلیٹ ہوا ہے، اسی میں انسٹال کرنے سے ڈیٹا مکمل طور پر ضائع ہوسکتا ہے۔

www.abyssalsoft.com/abyssal-recovery

EPUB فارمیٹ کی کتب فائر فاکس میں پڑھیں

اسمارٹ فونز اور ٹیبلٹس نے ایسی مقبولیت پائی ہے کہ اس نے کتب پڑھنے کی رجحان میں بھی زبردست تبدیلی پیدا کردی ہے۔ اب لوگ طبعی کتابیں پڑھنے کے بجائے اپنے اسمارٹ فونز اور ٹیبلٹس پر کتب پڑھنے کو ترجیح دیتے ہیں۔ یہ ترجیحات کی تبدیلی ہی ہے کہ اسمارٹ فونز اور ٹیبلٹس کے علاوہ کتب پڑھنے کے لئے مخصوص ڈیوائسز مثلاً Kindle بھی بنائی گئی ہیں۔ کینڈل کی مقبولیت کا اندازہ آپ اس بات سے لگا سکتے ہیں کہ اب تک اس کی تین نسلیں آچکی ہیں اور مجموعی طور پر لوگوں نے انہیں کروڑوں کی تعداد میں خریدا ہے۔

چونکہ پی ڈی ایف ڈاکیومنٹس اور دیگر فارمیٹ چھوٹی اسکرین کی ڈیوائسز پر پڑھنے کے لئے مناسب نہیں، اس لئے کچھ نئے فائل فارمیٹ متعارف کروائے گئے ہیں جن میں سے ایک EPUB یا الیکٹرانک پبلی کیشن ہے۔ یہ فارمیٹ کتابوں کے معاملے میں پی ڈی ایف جتنا ہی مقبول ہوگیا ہے اور اب کتب پی ڈی ایف کے ساتھ ساتھ EPUB فارمیٹ میں بھی پیش کی جاتی ہیں۔ EPUB فارمیٹ کی کتب کو پڑھنے کے لئے گوگل اینڈرائیڈ، بلیک بیری او ایس، ایپل آئی او ایس، ونڈوز فون سمیت دیگر اہم موبائل فون آپریٹنگ سسٹمز کے لئے مفت ایپلی کیشنز دستیاب ہیں۔

لیکن ضروری تو نہیں کہ آپ کے پاس EPUB فارمیٹ میں موجود کتاب پڑھنے کے لئے اسمارٹ فون بھی ہو۔ آپ چاہیں تو اس فارمیٹ کو فائر فاکس کے ذریعے کمپیوٹر پر بھی پڑھ سکتے ہیں۔

اس مقصد کے لئے آپ کو EPUB Reader نامی ایکسٹینشن درکار ہوگا۔ یہ ایکسٹینشن فائر فاکس کے لئے ہے۔ اسے انسٹال کرنے کے بعد آپ EPUB فارمیٹ کی کتب با آسانی فائر فاکس میں پڑھ سکتے ہیں۔ چونکہ اس ایکسٹینشن کا تعلق فائر فاکس کے ساتھ ہے، اس لئے ہر وہ آپریٹنگ سسٹم (ونڈوز، میک او ایس، لینکس وغیرہ) جس پر فائر فاکس انسٹال ہوسکتا ہے، یہ ایکسٹینشن بھی استعمال کیا جاسکتا ہے۔

http://www.epubread.com/en

مفت اکاؤنٹنگ سافٹ ویئر

اکاؤنٹنگ سافٹ ویئر اور وہ بھی مفت، ایک عجیب بات معلوم ہوتی ہے۔ اس کی وجہ یہ ہے کہ اکاؤنٹنگ سافٹ ویئر شاید وہ واحد سافٹ ویئر ہے جو پاکستان میں باقاعدہ بنایا، بیچا اور خریدا جاتا ہے۔ خیر، GnuCash اکاؤنٹنگ سافٹ ویئر صرف مفت ہی نہیں بلکہ اوپن سورس بھی ہے۔ ساتھ ہی یہ مائیکروسافٹ ونڈوز کے علاوہ لینکس اور میک او ایس کے لئے بھی مفت دستیاب ہے۔

GnuCash کے ذریعے ایک گھریلو اکاؤنٹنگ یا ایک چھوٹے کاروباری ادارے کی اکاؤنٹ کا کام بخوبی انجام دیا جاسکتا ہے۔ یہ ڈبل اینٹری اکاؤنٹنگ سسٹم کے تحت کام کرنے والا سافٹ ویئر ہے جو پاکستان سمیت دنیا بھر میں استعمال ہوتا ہے۔ مختلف رپورٹس اور چارٹس/گرافس بھی اس کے ذریعے تیار کئے جاسکتے ہیں جبکہ چیک پرنٹ کرنے کی سہولت بھی اس میں موجود ہے۔

GnuCash کے ساتھ استعمال کے لئے ایک اینڈرائیڈ ایپلی کیشن بھی موجود ہے۔

www.gnucash.org

ونڈوز کو میک او ایس ایکس یوسیمیٹی کے روپ میں ڈھالیں

ایپل میک او ایس ایکس کی شکل وصورت ونڈوز سے بہت مختلف ہے۔ چونکہ زیادہ تر لوگوں کو میک استعمال کرنے کو نہیں ملتا، اس لئے انہیں میک او ایس کے خوبصورت انٹرفیس کا دیدار بھی نہیں ہو پاتا۔ لیکن اس پریشانی کا بھی ایک آسان حل ہے۔ کیوں نہ ونڈوز کو ہی میک او ایس کا روپ دے دیا جائے؟

Yosemite Transformation Pack ایک ایسا ہی مفت سافٹ ویئر ہے جو مائیکروسافٹ ونڈوز کو میک او ایس کی شکل میں ڈھال دیتا ہے۔ دلچسپ بات یہ ہے کہ اسے ونڈوز ایکس پی سے لے کر ونڈوز 8.1 تک بشمول سرور ایڈیشن، میں انسٹال کیا جاسکتا ہے۔

Yosemite دراصل میک او ایس ایکس سیریز کا نیا آپریٹنگ سسٹم ہے جس کا اعلان ایپل نے اسی سال جون میں کیا تھا۔ توقع ہے کہ اس آپریٹنگ سسٹم کو باقاعدہ طور پر اس سال کے آخر میں جاری کردیا جائے گا۔ Yosemite Transformation Pack آپ کو اس آپریٹنگ سسٹم کی فائنل ریلیز سے پہلے ہی مائیکروسافٹ ونڈوز میں رہتے ہوئے اس کے مزے کرواسکتا ہے۔

دیگر ٹرانسفرمیشن پیکس کے مقابلے میں یہ اصل میک او ایس سے زیادہ قریب محسوس ہوتا ہے۔ نیز مائیکروسافٹ اپ ڈیٹس کی راہ میں یہ رکاوٹ بھی نہیں ڈالتا۔

دیگر ٹرانسفرمیشن پیکس کے ساتھ ہمیشہ سے یہ مسئلہ رہا ہے کہ انسٹالیشن کے بعد انہیں اگر uninstall کیا جائے تو وہ ونڈوز کو غیر مستحکم کردیتے ہیں یا کم از کم ونڈوز اپنی پہلی والی حالت میں نہ آپاتی تھی۔ یوسیمیٹی ٹرانفرمیشن پیک کے ساتھ یہ مسئلہ نہیں ہے۔ اسے انسٹال کریں، اگر پسند نہ آئے تو اَن انسٹال کردیں۔ اس عمل سے ونڈوز کو کوئی نقصان نہیں پہنچے گا۔ یاد رہے کہ اسے استعمال کرنے کے لئے ضروری ہے کہ آپ کے پاس مائیکروسافٹ ڈاٹ نیٹ فریم ورک 2.0 انسٹال ہو۔ اگر یہ انسٹال نہیں ہے تو آپ اسے مائیکروسافٹ کی ویب سائٹ سے مفت ڈاؤن لوڈ اور انسٹال کرسکتے ہیں۔

windowsxlive.net/yosemite-transformation-pack

دنیا بھر کھیل اسٹریمنگ کے ذریعے دیکھیں

دنیا بھر میں ہر روز مختلف کھیلوں کے مقابلے ہوتے رہتے ہیں جیسے کہ بیس بال، باسکٹ بال، سائیکلنگ، گالف، آئس ہاکی، رگبی وغیرہ۔ افسوس کی بات ہے کہ دنیا بھر میں مشہور یہ کھیل پاکستان میں براڈکاسٹ ہی نہیں ہوتے۔ حتیٰ کہ فٹ بال جیسے دنیا کے مقبول ترین کھیل کے کئی اہم میچ ہمارے ملک میں نہیں دکھائے جاتے۔ اگر آپ کسی بھی کھیل کا کوئی میچ لائیو بذریعہ انٹرنیٹ دیکھنا چاہیں تو اس کا بہترین طریقہ Ace اسٹریم پلیئر ہے۔ اس پلیئر کی مدد سے آپ کھیلوں کے علاوہ دیگر بھی کئی ٹی وی چینلز کو بذریعہ انٹرنیٹ دیکھ سکتے ہیں۔ اگر آپ کے پاس انٹرنیٹ کی اچھی رفتار ہے تو ہائی ڈیفی نیشن ٹی وی بھی دیکھ سکتے ہیں۔ Ace اسٹریم پلیئر ڈاؤن لوڈ کریں: acestream.org

کھیلوں کے اسٹریمنگ لنکس یہاں سے حاصل کریں:

www.wiziwig.tv

جی برنر کے ذریعے ورچوئل ڈرائیوز بنائیں

اکثر آپ انٹرنیٹ سے ISO فائلیں ڈاؤن لوڈ کرتے ہیں جنہیں سی ڈی یا ڈی وی ڈی پر burn کرنے کے بعد چلانا پڑتا ہے۔ اسی طرح کئی سافٹ ویئر خاص طور پر ویڈیو گیمز اپنی اصل سی ڈی/ ڈی وی ڈی کے بغیر چلتے ہی نہیں۔ لیکن یہ بات کئی لوگ نہیں جانتے کہ آپ ورچوئل ڈرائیوز بنا کر ان میں ISO سمیت کئی دیگر سی ڈی/ ڈی وی ڈی امیج فارمیٹس کو mount کر سکتے ہیں۔ یہ بالکل ویسا ہی ہے جیسے آپ سی ڈی یا ڈی وی ڈی ڈرائیو میں سی ڈی لگاتے ہیں۔

gBurner ورچوئل ڈرائیوز بنانے کے لئے ایک زبردست سافٹ ویئر ہے۔ یہ مفت بھی ہے اور تقریباً دو درجن امیج فارمیٹس جن میں BIN، UIF، NRG، ISO اور IMG جیسے معروف فارمیٹس بھی شامل ہیں، کو سپورٹ کرتا ہے۔ جی برنر کے ذریعے آپ 16 ورچوئل ڈرائیوز بنا سکتے ہیں جو کہ مائی کمپیوٹر میں دیگر ڈرائیوز کی طرح نظر آتی ہیں اور کام بھی ویسے ہی کرتی ہیں۔

وہ ویڈیو گیمز جو سی ڈی/ ڈی وی ڈی سے براہ راست چلتے ہیں، کی ڈسک کا امیج بنا کر ورچوئل ڈرائیو میں ماؤنٹ کرنے سے وہ گیم زیادہ تیز رفتاری سے چلتے ہیں۔

جی برنر کا دعویٰ ہے کہ ایسے ویڈیو گیمز 200 گنا جی ہاں، دوسو گنا تیز رفتاری سے لوڈ ہوتے ہیں۔ اس کی وجہ بھی سادہ سی ہے۔ سی ڈی/ ڈی وی ڈی ڈرائیو ڈسک سے ڈیٹا سست رفتاری سے پڑھتی ہیں جبکہ ہارڈ ڈسک اس کے مقابلے میں بہت تیز رفتار ہوتی ہے۔

gburner.com/online-help/virtual-drive.htm

خفیہ فائلوں کو چھپانے کا ایک خفیہ طریقہ

DeEgger بہت ہی دلچسپ سافٹ ویئر ہے۔ اس کے ذریعے آپ کسی خفیہ فائل کو کسی دوسری فائل میں محفوظ کر سکتے ہیں۔ فرض کریں کہ آپ کے پاس پاس ورڈز پر مشتمل ایک نوٹ پیڈ کی فائل ہے۔ آپ اس نوٹ پیڈ کی فائل کو کسی تصویر میں محفوظ کر سکتے ہیں۔ مزے دار بات یہ ہے کہ اس عمل سے اس دوسری فائل کو کوئی نقصان نہیں پہنچتا جس میں پہلی فائل محفوظ کی گئی ہے۔ محفوظ کی گئی خفیہ فائل کو واپس حاصل کرنے کے لئے بھی آپ کو اسی سافٹ ویئر کی ضرورت ہوگی۔ جس فائل کو محفوظ کرنا ہے وہ کوئی بھی فائل مثلاً کوئی آڈیو، ویڈیو، تصویر، ٹیکسٹ یا ڈاکیومنٹ ہوسکتی ہے، لیکن جس فائل میں اسے چھپانا ہے (اسے ہوسٹ فائل کہا جاتا ہے) کے لئے ضروری ہے کہ وہ html یا txt نہ ہو۔ تقریباً تمام آڈیو، ویڈیو اور تصویری فارمیٹس بطور ہوسٹ فائل قابل قبول ہیں۔

یہ بات نوٹ کر لیجئے کہ یہ ٹول ایک پرائیویسی ٹول تو ہوسکتا ہے لیکن ایک سکیوریٹی ٹول نہیں۔ بائنری کوڈ کی معلومات رکھنے والا کوئی بھی ہوشیار شخص خفیہ فائل کو ہوسٹ فائل سے نکال سکتا ہے۔ لیکن اتنے ہوشیار لوگ بہرحال کم ہی ہوتے ہیں۔ اس لئے عام استعمال کے لئے یہ دلچسپ سافٹ ویئر استعمال کرنے میں کوئی حرج نہیں۔ اسے ونڈوز ایکس پی سے ونڈوز 8.1 تک پر استعمال کیا جاسکتا ہے۔

www.zasi.org/DeEgger-Embedder.php

اسٹوڈیولائن فوٹو بیسک......ایسا فوٹو ایڈیٹر جس کی آپ کو تلاش تھی

تصاویر پر گرافکس ایڈیٹنگ سبھی کا پسندیدہ کام ہے۔ اگر آپ کو اپنی پسند کا کبھی کوئی امیج ایڈیٹر نہیں ملا، جو تصویر پر آپ کی پسند کے ایفیکٹس اور فلٹرز لگا سکے، یا آپ زیادہ گرافکس کی معلومات نہیں رکھتے اور صرف اپنی تصویر کو بہتر بنانا چاہتے ہیں تو ''اسٹوڈیولائن'' کا ''فوٹو بیسک'' آپ ہی کے لیے ہے۔

اسٹوڈیولائن کا پروگرام ''فوٹو کلاسک'' اپنی لاجواب کارکردگی کی وجہ سے بہت تیزی سے مقبول ہورہا ہے لیکن یہ پروگرام قیمتاً دستیاب ہے۔ جو لوگ اسے خریدے بنا استعمال کرنا چاہیں ان کے لیے کلاسک ورژن کی کانٹ چھانٹ کر کے کچھ ہلکا ورژن بیسک کے نام سے فراہم کیا گیا ہے۔ اسے صرف بنیادی سا فوٹو ایڈیٹر سمجھ کر درگزر نہ کریں، کیونکہ یہ ایک مکمل فوٹو ایڈیٹر کی تمام صلاحیتوں کا حامل ہے۔

تاہم، پروگرام صرف فوٹو ایڈیٹر ہی نہیں، ایک منیجمنٹ ٹول بھی ہے۔ آپ جن جن فولڈرز سے چاہیں تصاویر اس میں ایک جگہ جمع کر سکتے ہیں۔ اس کے ذریعے آپ اپنی تمام تصاویر کو ورڈز اور ڈسکرپشن کے ساتھ منظم رکھ سکتے ہیں۔ اس طرح ضرورت پڑنے پر تصاویر کو آسانی کے ساتھ تلاش کیا جاسکتا ہے۔

فوٹو بیسک میں تصاویر کے حوالے سے لاتعداد فیچرز موجود ہیں جیسے کہ تصاویر کا سائز بدلنا، انھیں گھمانا، تصویر میں آنکھوں کی لال پتلی ٹھیک کرنا وغیرہ۔ تصاویر کی کوالٹی بہتر کرنا اور ان پر دلکش ایفیکٹس اپلائی کر کے انھیں دلکش بنانا سب کچھ اس میں موجود ہے۔ فوٹو بیسک میں درجنوں ایفکٹس اور فلٹرز موجود ہیں۔ اس پروگرام سے آپ تصویری گیلری بنا سکتے ہیں اور تصویروں کی سلائیڈ شو بھی بنا سکتے ہیں۔ اس کے علاوہ اس کی مدد سے تصاویر کو پرنٹ، اپ لوڈ کے علاوہ سی ڈی اور ڈی وی ڈی پر بھی چند کلکس سے محفوظ کیا جاسکتا ہے۔

اگر آپ کی فوٹوگرافی میں کوئی کمی رہ گئی ہو تو اپنی تصویر کو اس پروگرام سے گزاریں۔ تصویر میں جو خرابی ہو اس کی مدد سے درست کر کے دوستوں سے شیئر کریں۔ تصویر پر کام کرنے کے لیے امپورٹ کے بٹن پر کلک کرتے ہوئے تصویر منتخب کرلیں۔ اس کے علاوہ تصویر ڈریگ اینڈ ڈراپ کے ذریعے بھی اس میں لائی جاسکتی ہے۔ ''ایڈٹ ٹولز'' سے تصویر پر بنیادی کام کیا جا سکتا ہے۔ جبکہ نیچے موجود بار کے ذریعے تصویر کا سائز بدلا جا سکتا ہے۔ دیگر ایڈوانسڈ تبدیلیاں کرنے کے لیے امیج ٹولز بٹن پر کلک کریں۔ یہ آپشن کھلنے کے بعد سامنے ہی نظر آتا رہتا ہے اس لیے کام مکمل کرنے کے بعد اسے کلوز کردیں۔ تمام کام کے دوران اصل تصویر بھی محفوظ رکھی جاتی ہے آپ دونوں تصویروں کا موازنہ کرسکیں۔ اس پروگرام میں بہت خوبصورت ایفیکٹس موجود ہیں، جن کو استعمال کرتے ہوئے آپ اپنی تصویروں کی دلکشی باآسانی بڑھا سکتے ہیں۔

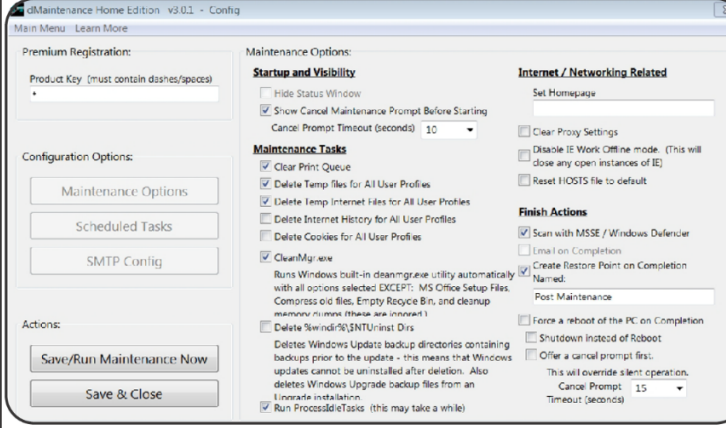
اگرچہ پروگرام بالکل مفت دستیاب ہے لیکن تیس دن کے استعمال کے بعد آپ کو ایکٹی ویشن کوڈ کی درخواست دینا پڑتی ہے جو کہ مفت فراہم کیا جاتا ہے۔

فائل سائز: 47.7 MB

studioline.net/en/downloads/photo-basic

ایکٹی ویشن کوڈ حاصل کرنے کے لیے درج ذیل ربط پر جائیں:

store.studioline.net/?Document=Activate.asp

آپ کی ضرورت کے تحت سسٹم مینٹیننس ......صرف ایک کلک سے!

کام کرتے کرتے اگر کمپیوٹر سست پڑنے لگے تو انتہائی اُلجھن ہوتی ہے۔ اس کے علاوہ اگر فالتو فائلز کی وجہ سے اسپیس استعمال ہو رہی ہو، پرنٹر میں پرنٹس رُکے ہوں، انٹرنیٹ ایکسپلورر آف لائن موڈ میں چلا گیا ہو یا اس پر کسی پروگرام نے پراکسی سیٹنگز خود بخود سیٹ کر کے آپ کا انٹرنیٹ سے رابطہ ہی منقطع کر دیا ہو یا پھر سب سے بڑھ کر سسٹم پر وائرس تشریف لا چکے ہوں یہ سارے مسئلے انتہائی اُلجھن میں مبتلا کر دیتے ہیں۔ اگر ایسا مسئلہ آپ نے کافی دن سے نہیں بھی دیکھا تو پھر بھی سسٹم کو کچھ دن بعد تھوڑی صفائی ستھرائی کی ضرورت ہوتی ہے، تا کہ اس کی کارکردگی برقرار رہے۔ ''ڈی مینٹیننس ہوم ایڈیشن'' پروگرام اس کام کے لیے بالکل مفت دستیاب ہے۔ اپنے کام کے حوالے سے یہ ایک انتہائی طاقت ور اور برق رفتار پروگرام ہے۔ اوپر بتائے گئے تمام مسائل سے نمٹنے کے معاملے میں یہ کسی قسم کی کوتاہی نہیں برتتا۔ بلکہ اسے صرف حکم دینے کی دیر ہوتی ہے، باقی سارے کام یہ خود بخود کر دیتا ہے۔ جو جو کام درکار ہوں صرف انھیں بھی منتخب کیا جا سکتا ہے۔ اس کے علاوہ کام ہونے کے بعد پروگرام کیا کرے، یہ کنفگریشن کرنے کے بعد یہ پروگرام ایک خود کار ٹول میں بدل جاتا ہے جو ون کلک پر اپنی ذمے داری ادا کرتا رہتا ہے۔

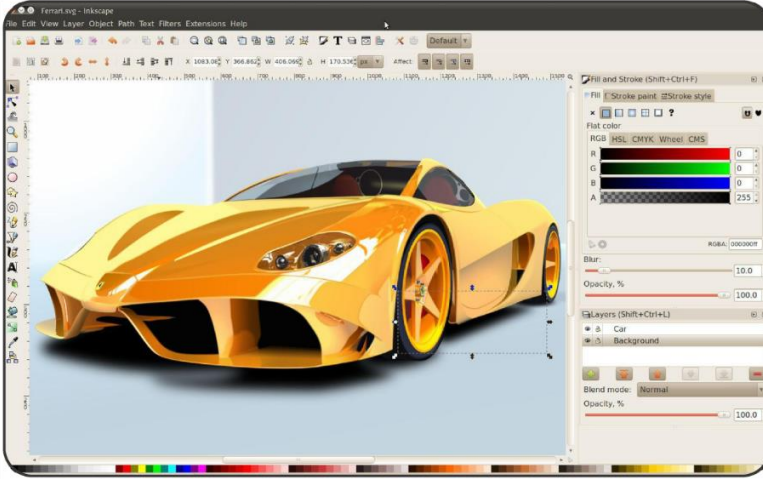
فائل سائز: 771KB　　مطابقت: ونڈوز تمام ورژنز

foolishit.com/dmaintenance-home-edition

سسٹم کی خرابی کی صورت میں نقصان سے بچیں

ڈیٹا ریکوری کے حوالے سے ''پیراگون'' ایک جانا مانا نام ہے۔ پیراگون کی جانب سے فراہم کردہ ''ریسکیو کٹ'' بہت کام کی چیز ہے۔ ایک خراب سسٹم جو بالکل بوٹ نہ ہو پا رہا ہو، یہ پروگرام بوٹ نہ ہونے کی وجہ بننے والے عام مسائل کو ٹھیک کرنے کے قابل ہے۔ اس کے علاوہ سسٹم کی خرابی کی وجہ سے یہ ڈیٹا کو ضائع ہونے سے بچا سکتا ہے۔ غلطی سے ڈیلیٹ ہو جانے والے پارٹیشن سے ڈیٹا اس پروگرام کی مدد سے نکالا جا سکتا ہے۔ کسی بھی خطرے سے پیشگی تیار رہنے کے لیے یہ ٹول کٹ آپ کے پاس موجود ہونی چاہیے۔ تاکہ کسی بھی ناگہانی کی صورت میں اپنا قیمتی ڈیٹا بروقت حاصل کر سکیں۔ پروگرام میں موجود ریسکیو وزارڈ کمپیوٹر کے خراب ہونے کی صورت میں نقصان سے بچاتا ہے۔ کیونکہ اس میں بوٹ کریکٹر، ان ڈیلیٹ پارٹیشن، رجسٹری ایڈیٹر، پاس ورڈ کلینر، لاگ سیور جیسے بہترین فیچرز موجود ہیں۔ اس کٹ کو سی ڈی یا یو ایس بی کے ذریعے جیسے چاہیں استعمال کیا جا سکتا ہے۔ ونڈوز ایٹ کی مطابقت بھی اس میں موجود ہے۔ پروگرام کو استعمال کرنے کے لیے مفت دستیاب پروڈکٹ کی اور سیریل نمبر چاہیے ہوتا ہے۔

paragon-software.com/home/rk-free

اِنک اسکیپ......ایک اوپن سورس ویکٹر گرافکس ایڈیٹر

ویکٹر گرافکس کی بات کی جائے تو سب سے پہلے کورل ڈرا یا ایڈوبی السٹریٹر کا نام ہی ذہن میں آتا ہے۔ اس کے ساتھ ساتھ یہ بھی ذہن میں آنا چاہیے کہ یہ پروگرامز مفت دستیاب نہیں۔ ان کا ایک بہترین مفت متبادل ''انک اسکیپ'' کے نام سے موجود ہے۔ بلکہ اپنی کارکردگی کی بنا پر یہ پروگرام کورل ڈرا اور السٹریٹر کو کڑی ٹکر دیے ہوئے ہے۔

اسٹائلش لوگو ڈیزائن کرنے ہوں، ویب گرافکس بنانی ہو، کلپ آرٹ ہو یا تکنیکی ڈایا گرامز ویکٹر گرافکس کے حوالے سے کسی بھی کام کے لیے آپ انک اسکیپ کو استعمال کر سکتے ہیں۔

اس پروگرام کی خاص یہ ہے کہ یہ ونڈوز کے علاوہ لینکس و میک آپریٹنگ سسٹمز کے لیے بھی بالکل مفت دستیاب ہے۔ علاوہ ازیں اس کا سورس کوڈ بھی اس کی ویب سائٹ پر موجود ہے۔ جسے بلا معاوضہ نہ صرف ڈاؤن لوڈ کیا جا سکتا ہے بلکہ اگر آپ سافٹ ویئر ڈیویلپر ہیں تو اس میں تبدیلیاں بھی کر سکتے ہیں۔

اگر آپ اس پروگرام کو استعمال کرنا سیکھنا چاہیں تو ویب سائٹ پر باقاعدہ ٹیوٹوریل بھی دستیاب ہیں۔

www.inkscape.org/en

مووی کلپس کو آن لائن شیئر کرنے کے لیے جِف تصاویر میں کنورٹ کریں

چند سیکنڈ کے وڈیو کلپ کو جِف (Gif) تصویر میں بدلنا ایک دلچسپ کام ہوتا ہے۔ کیونکہ وڈیو کے مقابلے میں جِف (Gif) تصاویر کو مختلف ویب سائٹس پر اور دوستوں سے شیئر کرنا زیادہ آسان ہوتا ہے۔

اگر آپ بھی کسی وڈیو سین کو جف فائل میں کنورٹ کرنا چاہتے ہیں تو ''مووی ٹو جف'' نامی یہ سافٹ ویئر مفت ڈاؤن لوڈ کر کے استعمال کر سکتے ہیں۔ اسے استعمال کرنے کا طریقہ کار انتہائی سادہ اور آسان ہے۔ جو سین جف میں کنورٹ کرنا ہو پہلے اس کی وڈیو یا فلم اس پروگرام میں کھول لیں۔ اس کے بعد وہ حصہ منتخب کریں جس کی جف بنانی ہو۔ یعنی آپ کو آغاز اور ابتدا کے مقام کی نشاندہی کرنی ہوگی۔ اس کے بعد اسے Save as GIF کر لیں، آپ کی فائل تیار ہو جائے گی۔

جف فائل بناتے ہوئے اپنی پسند کی سیٹنگز بھی سرانجام دی جا سکتی ہیں جیسے کہ سائز، اسپیڈ، فریم ریٹ اور کلر وغیرہ۔ وڈیو فارمیٹس کی سپورٹ کی بات کی جائے تو یہ قریباً تمام معروف وڈیو فارمیٹس جیسے کہ MKV، WMV، MP4، MPEG، AVI، MOV اور VOB کی سپورٹ کا حامل ہے۔

en.zxt2007.com/video-tools/movietogif.html

جانیے آپ کی غیر موجودگی میں کمپیوٹر پر کیا کچھ کیا گیا

آج کل تقریباً سبھی کے پاس اپنا ذاتی کمپیوٹر یا لیپ ٹاپ ہوتا ہے۔ چونکہ اسے کسی کے ساتھ شیئر نہیں کرنا ہوتا اس لیے ہم اپنا ذاتی ڈیٹا جہاں چاہیں رکھ سکتے ہیں۔ اگر کبھی کمپیوٹر کسی دوسرے کو استعمال کے لیے دینا پڑ جائے تو ''او ایس فرونسکس'' سافٹ ویئر کے انسٹال ہونے سے آپ مکمل طور پر جان سکتے ہیں کہ کمپیوٹر پر کیا کیا گیا۔ یہ مکمل رپورٹ فراہم کرتا ہے کہ کون سی ویب سائٹ دیکھی گئی، کیا ڈاؤن لوڈ کیا گیا، کون سی یو ایس بی فلیش ڈرائیو سسٹم کے ساتھ لگائی گئی، کون کون سی فائلیں کھولی گئیں یا تلاش کی گئیں وغیرہ۔ اس طرح کی مکمل رپورٹ آپ کو ایک کلک کی خبر دیتی ہے۔

اس کے تازہ ورژن میں مزید کئی خوبیاں شامل کی گئی ہیں جو واقعی میں ایک مکمل رپورٹ بنانے میں مدد دیتی ہیں مثلاً یہ پروگرام یہ بات تک نوٹ کرتا ہے کہ کون کون سے پروگرام استعمال کیے گئے اور وہ بھی کتنی بار یا کتنی دیر تک۔

اس میں موجود تھمب کیشے ویور کی مدد سے ایکسپلورر کی تھمب نیل تصاویر بھی دیکھی جاسکتی ہیں لیکن یہ آپشن ونڈوز ایکس پی کے لیے دستیاب نہیں۔ اسے استعمال کرنے کے لیے آپ کے پاس ونڈوز وستا یا اس سے بعد کا کوئی آپریٹنگ سسٹم جیسے کہ ونڈوز سیون یا ایٹ ہونی چاہیے۔

فائل سائز: 43.31MB

www.osforensics.com

صرف ایک کلک اور سست پڑتی ڈیوائس چست

اگر کبھی محسوس ہو کہ کمپیوٹر سست پڑ رہا ہے تو ہم کچھ فالتو پروگرامز بند کر کے، فالتو فائلز وغیرہ ڈیلیٹ کر کے اس کی رفتار کو معمول پر لانے کی کوشش کرتے ہیں۔ اگر آپ اس معاملے میں ماہر نہیں تو یقیناً آپ کو ایک اچھا سافٹ ویئر درکار ہوگا۔ اس کام کے لیے ''ریمومور'' کے نام سے ایک بہترین ایپلی کیشن موجود ہے۔ اس پروگرام کی خاص بات اس کا ونڈوز کے علاوہ میک، اور اینڈرائیڈ و آئی او ایس کے لیے بھی دستیاب ہونا ہے۔

ریمومور کی شاندار بات اس کا کلاؤڈ بیسڈ ہونا ہے۔ یعنی اپنی تمام ڈیوائسز کو آپ ایک اکاؤنٹ میں جمع کر کے ان پر ریموٹلی ریمومور کو استعمال کرتے ہوئے سسٹم یا ڈیوائس کی خرابیاں درست کر سکتے ہیں، اس کے ہارڈ ویئر کی مکمل رپورٹ، بیٹری اسٹیٹس جان سکتے ہیں۔ کمپیوٹر ہارڈ ڈسک سے لے کر آئی فون اور اینڈرائیڈ کے ڈائگنوسٹکس تک کے لیے اس میں ٹولز موجود ہیں۔ اس کے علاوہ یہ انٹرنیٹ کنکشن تک کو بہتر بنانے میں مددگار ثابت ہوتا ہے۔ اس پروگرام میں اتنے فیچرز موجود ہیں کہ چند پیروں میں بیان کرنا ممکن نہیں۔ آل اِن ون ریمومور کی مدد سے آپ پی سی ایررز کو ٹھیک کر سکتے ہیں، سی پی یو اور ریم کا استعمال درست کر سکتے ہیں، ذاتی ڈیٹا انکرپٹ کر سکتے ہیں اور آرکائیو فائلز بھی بنا سکتے ہیں۔

www.remosoftware.com/domore

اپنی فیس بک ڈی پی کی ڈرائنگ کروائیں

selflessportraits.com

یوں تو کئی ایسی مفت ویب سائٹس موجود ہیں جہاں آپ اپنی تصاویر کو ہاتھ سے بنائی ہوئی ڈرائنگ جیسا ایفیکٹ دے سکتے ہیں۔ لیکن کسی مصور سے اپنی تصویر کی ڈرائنگ بنوانا عموماً مفت نہیں ہوتا۔ سیلف لیس پورٹریٹس ایک ایسی ویب سائٹ ہے جہاں دنیا بھر سے سینکڑوں، ہزاروں آرٹسٹ دوسروں کی تصاویر کو اسکیچز اور پینٹنگز میں بدلتے ہیں اور وہ بھی بالکل مفت!

سیلف لیس پورٹریٹس پر صرف فیس بک پر اپ لوڈ کی گئی تصاویر کو ہی ڈرائنگز یا اسکیچز بنانے کے لئے پیش کیا جاسکتا ہے، یعنی آپ اس ویب سائٹ پر اپنی مرضی سے تصاویر اپ لوڈ نہیں کرسکتے۔

اگر آپ بھی اپنے فیس بک ڈی پی کو پینٹنگ میں بدلنا چاہتے ہیں تو اس ویب سائٹ پر موجود Participate کے بٹن پر کلک کریں۔ یہ ویب سائٹ آپ سے اجازت لینے کے بعد خود ہی آپ کے فیس بک اکاؤنٹ سے تصاویر نکال لاتی ہے۔

چونکہ تصاویر کو اسکیچز اور پینٹنگز میں بدلنے کا کام مکمل طور پر اجنبی رہ کر کیا جاتا ہے اس لئے کئی بار نتیجہ آپ کی مرضی کا نہیں ہوتا۔ کچھ آرٹسٹ پینسل سے اسکیچ بناتے ہیں جبکہ کچھ اس کام کے لئے کمپیوٹر کا استعمال کرسکتے ہیں۔ اسی طرح پینٹنگ یا ڈرائنگ میں آپ کی شکل وصورت کو بھی آرٹسٹ عجیب وغریب بنا سکتا ہے۔

فونٹ بنانا سیکھئے

practicaltypography.com

خوبصورت فونٹ استعمال کرنا کسے پسند نہیں۔ لیکن اگر آپ خطاطی میں دلچسپی رکھتے ہیں یا اپنی لکھائی کو فونٹ میں بدلنا چاہتے ہیں تو یہ ویب سائٹ آپ کے لئے ایک اچھا آغاز ثابت ہوگی۔ یہاں آپ فونٹ بنانے کے لئے درکار ضروری معلومات حاصل کرسکتے ہیں۔ فونٹ کی اقسام، glyphs، kerning، پوائنٹ سائز، فونٹ فیملی جیسے موضوعات کو اس ویب سائٹ پر عملی انداز میں سکھایا گیا ہے۔ یہاں فونٹ بنانے کی کوئی ترکیب موجود نہیں، لیکن فونٹ بنانے کے لئے جو بھی بنیادی معلومات چاہئے ہوتی ہے، وہ یہاں سے آسان اور عملی انداز میں سیکھی جاسکتی ہے۔

BUTTERICK'S
PRACTICAL
TYPOGRAPHY

INTRODUCTION
how to use this book

WHY TYPOGRAPHY MATTERS
what is typography?
who is typography for?
why does typography matter?

TYPE COMPOSITION
straight and curly quotes
one space between sentences
question marks and exclamation points
semicolons and colons
paragraph and section

topsy.com

آٹھ سال پرانی ٹویٹس تلاش کیجئے

ٹوئٹر 2006ء میں انٹرنیٹ پر وارد ہوا تھا اور تب سے یہ سوشل میڈیا کا ایک اہم جز ہے۔ دنیا بھر میں اسے کروڑوں لوگ روزانہ استعمال کرتے ہیں۔ ٹوئٹر کے صارفین اپنی اور دیگر صارفین کی پوسٹ کی ہوئی ٹویٹس کو سرچ کر سکتے ہیں۔ لیکن سرچنگ کا یہ عمل صرف کچھ عرصہ پہلے کی گئی ٹویٹس تک محدود ہوتا ہے۔ یعنی آپ چند ماہ پرانی ٹویٹس تو سرچ کر سکتے ہیں لیکن سال 2009ء میں کی گئی ٹویٹس کے بارے میں نہیں جان سکتے۔ ایک اندازے کے مطابق 2006ء سے اب تک تقریباً پانچ سو ارب (500 ارب) ٹویٹس کی جا چکی ہیں۔ topsy ویب سائٹ پر 2006ء کے بعد سے اب تک کی جانے والی تمام ٹویٹس کو تلاش کیا جاسکتا ہے۔ یہ ڈیٹا جرنلزم (اعداد و شمار کی بنیاد پر رپورٹنگ) اور ڈیٹا سائنٹسٹ کے لئے کسی خزانے سے کم نہیں جو آج سے سات سال پہلے ہونے والے کسی واقعے کے بارے میں لوگوں کے تاثرات یا واقعے کی تفصیل دنیا بھر کے لوگوں سے جاننا چاہتے ہیں۔

topsy پر ایک سے زیادہ کی ورڈز اور ہیش ٹیگز کا تجزیہ بھی کیا جاسکتا ہے۔ اس سے پتا چلایا جاسکتا ہے کہ کون سا ہیش ٹیگ زیادہ مقبول ہے اور کون سے دن اس کے بارے میں زیادہ ٹویٹس کی گئیں۔ اسی طرح مقبول ٹرینڈز کے بارے میں بھی زبردست ڈیٹا حاصل کیا جاسکتا ہے۔ صحافی حضرات اور ریسرچرز کے لئے ہم یہ ویب سائٹ خاص طور پر تجویز کریں گے۔

countryreports.org

ہر ملک کی معلومات، ایک ویب سائٹ پر

اگر آپ کو سیاحت کا شوق ہے یا آپ گھر بیٹھے مختلف ملکوں کی سیر، وہاں کے رسم و رواج، ثقافت اور زبان کے بارے میں جاننا چاہتے ہیں تو پھر کنٹری رپورٹ آپ کے لئے ایک بہترین ویب سائٹ ہے۔ اس ویب سائٹ پر آپ کی دلچسپی کے لئے تقریباً پینتیس ہزار (35000) صفحات موجود ہیں۔

بیرون ملک سفر کرنے والے افراد کے لئے اس ملک کے رسم و رواج سمیت کئی چیزوں کے بارے میں جاننا بے حد ضروری ہوتا ہے۔ بصورت دیگر مالی اور جسمانی نقصان کا اندیشہ رہتا ہے۔ مثلاً اگر آپ برازیل کا سفر کر رہے ہیں تو کسی بھی فٹ بال کلب یا ٹیم کی شرٹ پہن کر ہرگز مت گھومیں کیونکہ برازیلی اس معاملے میں بے حد حساس ہیں۔ کچھ ایسی ہی تجویز فٹ بال کے شیدائی دیگر ممالک کے لئے بھی دی جاتی ہے۔

کنٹری رپورٹ پر آپ دنیا کے کسی بھی ملک کی تاریخ، فیشن، کھانے اور ان کی اہم ترکیبیں، کھیل، مذہب، سیاست، شماریات، جغرافیہ، زراعت، اہم تجارتی پیشے، آب و ہوا، ملک کا نقشہ، کرنسی، قوانین، درآمدات و برآمدات، معیشت، زبان، اہم حکومتی اداروں کے پتے و ٹیلی فون نمبرز کی معلومات چند منٹوں میں حاصل کر سکتے ہیں۔ اس کے علاوہ کسی ملک کے مرد و عورتوں کا رہن سہن، وہاں کے تاریخی و تفریحی مقامات کا بھی تفصیلی ذکر موجود ہے۔ غرض یہ کہ یہاں کسی بھی ملک کے بارے میں الف تا ے معلومات با آسانی مل جاتی ہے۔ تمام معلومات خوبصورت تصاویر کے ساتھ پیش کی جاتی ہیں جس سے یہ ویب سائٹ مزید جاذب نظر ہو جاتی ہے۔ بچے، بوڑھے، مرد و خواتین، سیاحوں، بین الاقوامی منڈیوں کے تاجروں اور طلباء اس ویب سائٹ سے بھرپور فائدہ اٹھا سکتے ہیں۔ کنٹری رپورٹ کسی بیش قیمت خزانے سے کم نہیں۔ (ایمن جاوید، کراچی)

یہ فونٹ کون سا ہے؟

myfonts.com/WhatTheFont/

گرافکس ڈیزائنرز کو اکثر ایک پریشانی کا سامنا رہتا ہے کہ کسی تصویر میں موجود متن (ٹیکسٹ) کو ٹائپ کرنے کے لئے کون سا فونٹ استعمال کیا گیا ہے۔ خاص طور پر یہ پریشانی اس وقت اور بڑھ جاتی ہے جب استعمال کیا گیا فونٹ مقبول اور عام نہ ہو۔ ایسے میں متبادل فونٹ تلاش کرنا کسی عذاب سے کم نہیں۔ WhatTheFont اس پریشانی کا حل ہے۔ بس تصویر اپ لوڈ کیجئے اور یہ ٹول چند ہی لمحوں میں تصویر کا تجزیہ کرکے آپ کو بتادے گا کہ تصویر میں استعمال کیا گیا فونٹ کون سا ہے۔ یاد رہے کہ اپ لوڈ کی گئی تصویر میں ٹیکسٹ جتنا صاف ستھرا اور واضح ہوگا، نتیجہ بھی اتنا ہی بہترین ہوگا۔

اگر تصویر پہلے ہی انٹرنیٹ پر موجود ہو تو آپ اسے اپنے پاس ڈاؤن لوڈ کرکے یہاں اپ لوڈ کرنے کے بجائے براہ راست اس کا یو آر ایل بھی دے سکتے ہیں۔ یہ ویب سائٹ خود ہی اس تصویر کو ڈاؤن لوڈ کرکے اس کا تجزیہ کرلے

گی۔ فونٹ کے بارے میں رائے دینے سے پہلے ویب سائٹ تصویر میں سے کچھ حروف شناخت کرکے آپ سے انہیں ٹائپ کرنے کو بھی کہتی ہے۔

کامکس بنائیں

stripcreator.com

سوشل میڈیا پر کامکس (comics) انتہائی مقبول ہیں اور نیوز فیڈ، ٹوئٹر اسٹریم کا ایک بڑا حصہ مزاحیہ اور دلچسپ کامکس سے بھرا ہوتا ہے۔ انہیں بنانے میں خاصی دماغ سوزی کرنی پڑتی ہے۔ لیکن یہ ایک دلچسپ مشغلہ ہے۔

اسٹرپ کری ایٹر کامکس بنانے کے لئے ایک بہترین آن لائن ٹول ہے۔ اس کے ذریعے آپ چند منٹوں میں دلچسپ کامک کرسکتے ہیں۔ یہ آپ کو مختلف کریکٹرز، بیک گراؤنڈز سمیت دیگر ضروری سیٹنگز فراہم کرتا ہے تاکہ آپ اپنی مرضی ومنشاء کے مطابق کامک تیار کرسکیں۔ کامک کو محفوظ بنانے کے لئے آپ کو یہاں اکاؤنٹ بنانا ہوگا جو کہ بالکل مفت ہے۔ اگر کامکس میں آپ کی دلچسپی بہت زیادہ ہے تو اس ویب سائٹ کی آپ کو لت بھی لگ سکتی ہے!

انگریزی الفاظ کی تاریخ

etymonline.com

انگریزی ایک وسیع زبان ہے جسے ایک عالمی زبان کی حیثیت حاصل ہوچکی ہے۔ لیکن دیگر کئی زبانوں کی طرح انگریزی بھی ارتقاء کے عمل سے گزر کر آج اس مقام پر پہنچی ہے۔ اس میں شامل کئی الفاظ دیگر زبانوں سے لئے گئے ہیں جبکہ کئی الفاظ اپنی اصل شکل وصورت کھو چکے ہیں۔ مثلاً لفظ example دراصل قدیم فرانسیسی لفظ essemple سے اخذ کیا گیا ہے اور 13 ویں صدی میں اسے example نہیں بلکہ asaumple لکھا جاتا ہے۔ اسی طرح کئی الفاظ اپنے معنی تک تبدیل کرچکے ہیں۔ انگریزی الفاظ کی تاریخ اور ان کے مطلب کے بارے میں یوں تو کئی آن لائن لغات موجود ہیں لیکن etymonline ان میں سب سے زیادہ نمایاں ہے۔ یہ انتہائی جامع اور آسان ہے۔ انگریزی ادب کے طلباء کے لئے یہ خاص طور پر مفید ہے کیونکہ انگریزی ادب پر قدیم انگریزی کی چھاپ بہت گہری ہے۔ عام طلباء بھی اس سے انگریزی الفاظ کے بارے میں دلچسپ حقائق جان سکتے ہیں۔

funbrain.com

دماغی ورزش کیجئے

یہ ویب سائٹ بچوں سے لے کر بوڑھوں تک میں مشہور ہے اور ہر زبان میں ہر ملک کے رہنے والوں کی پسندیدہ ویب سائٹ ہے۔ اگر آپ کا یہ دعویٰ ہے کہ آپ بہت ذہین ہیں تو یہ ویب سائٹ آپ کے لئے ہی ہے۔ یہاں سیکڑوں کی تعداد میں ویڈیو گیمز، معمے اور سوال وجواب کے ساتھ ساتھ آپ کے سوچنے سمجھنے کی صلاحیت کو پرکھنے کے لئے پیچیدہ صورت حال والی پہیلیاں بھی موجود ہیں۔ ہمارا دعویٰ ہے کہ آپ اگر ایک بار اس ویب سائٹ پر تشریف لے گئے تو آپ کی دلچسپی کا یہاں اتنا سامان ہے کہ آپ کا اُٹھنا مشکل ہوجائے گا۔ یہ وقت گزاری کے لئے بھی اچھی جگہ ہے۔ لیکن یہاں وقت گزاری بھی آپ کو کئی دلچسپ چیزیں سکھانے کے علاوہ مزید ہوشیار بنائے گی۔

ایک تحقیق کے مطابق انسان کو سوچنا اور غور وفکر کرتے رہنا چاہئے کیونکہ اس سے دماغ صحت مند رہتا ہے اور اس کی فعالیت میں اضافہ ہوتا ہے۔ برین ڈاٹ کام دماغ کی ورزش کے لئے بہترین ویب سائٹ ہے جس کا مطلب ہے کہ یہ ویب سائٹ آپ کو ذہین اور چالاک بنا سکتی ہے۔ (ایمن جاوید، کراچی)

rasterbator.net

آن لائن پوسٹر بنائیں

ایک عام پرنٹر پر بڑے سائز کے پوسٹر پرنٹ کرنا ممکن نہیں۔ لیکن آپ اسکول، کالج یا یونی ورسٹی کا پروجیکٹ یا شوقیہ اپنی کسی تصویر کو ٹکڑوں میں کاٹ کر انہیں پرنٹ کر سکتے ہیں۔ لیکن یہ کام آسان نہیں۔ اس کام کو سہل بنانے کے لئے آپ راسٹربٹر ویب سائٹ کا استعمال کر سکتے ہیں۔ اس کا استعمال کسی ڈیسک ٹاپ سافٹ ویئر جیسا ہی ہے۔ بس اپنی مرضی کی تصویر اپ لوڈ کریں اور اسکرین پر ظاہر ہونے والی ہدایات کو بغور پڑھتے اور ان پر عمل کرتے رہیں۔ چند ہی لمحوں میں پی ڈی ایف فائل تیار کر کے آپ کو ڈاؤن لوڈنگ کے لئے پیش کردی جائے۔ اس پی ڈی ایف فائل میں تصویر ٹکڑوں کی شکل میں ہوگی جنہیں آپ با آسانی پرنٹ کر سکتے ہیں۔ آپ اگر چاہیں تو پوسٹر میں چند بصری اثرات (وژول ایفیکٹس) بھی شامل کر سکتے ہیں۔ جبکہ آپشنز کے ذریعے آپ پوسٹر کو مکمل طور پر پرنٹ کرنے کے لئے درکار صفحات کی تعداد کم زیادہ بھی کر سکتے ہیں۔

sleepyti.me

سونے کا اچھا وقت کون سا ہے؟

ویسے تو نیند کہیں بھی آسکتی ہے لیکن ماہرین کہتے ہیں کہ نیند کا وقت متعین کر کے اسی وقت سونا صحت کے لئے اچھا ہوتا ہے۔ sleepyti ویب سائٹ کے ذریعے آپ اپنے سونے اور جاگنے کا بہترین وقت معلوم کر سکتے ہیں۔ اس ویب سائٹ کے مطابق نیند کا پورا عمل مرحلہ وار ہوتا ہے اور ہر مرحلہ یا سائیکل 90 منٹ کا ہوتا ہے۔ ایک سائیکل سے دوسرے سائیکل کے درمیان اٹھنے سے ناگوار کیفیت طاری ہوجاتی ہے۔ لہٰذا اٹھنے کا بہترین وقت سائیکل کے اختتام پر ہے۔ مثلاً اگر آپ نے صبح 7 بجے اٹھنا ہے تو سونے کا سب سے اچھا وقت رات 10 بجے یا گیارہ بج کر تیس منٹ یا ایک بجے یا صبح کے ڈھائی بجے ہے۔ ان اوقات پر سونے سے آپ صبح 7 بجے اٹھنے پر ہشاش بشاش اٹھیں گے۔ یاد رہے کہ ایک عام انسان کو سونے کے لئے اوسطاً 14 منٹ درکار ہوتے ہیں۔

وی بی ڈاٹ نیٹ سیکھئے سلسلے کے گزشتہ حصے میں ہم نے ایک سادہ کیکولیٹر بنانا سیکھا تھا۔ ہم نے مرحلہ وار اس میں مختلف فیچرز کا اضافہ کیا، کچھ خامیاں دور کیں اور کچھ فنکشنز کے بارے میں بحث کی۔ آج ہم اس سلسلے کو مزید آگے بڑھاتے ہوئے لوپس (Loops) کا ذکر کریں گے۔

بعض اوقات ہمیں کسی کام کو بار بار کرنے کی ضرورت پیش آتی ہے۔ عموماً پروگرامنگ کوڈ سلسلہ وار چلتا ہے، کسی اسٹیٹمنٹ میں پہلے موجود فنکشن سب سے پہلے چلایا یا ایگزی کیوٹ کیا جاتا ہے اور اس کے بعد آنے والا کوڈ پہلے کے چل جانے کے بعد ایگزی کیوٹ ہوتا ہے۔ پروگرامنگ لینگویجز ہمیں مختلف طریقوں کے ذریعے اس کنٹرول اسٹرکچر کو تبدیل کرنے کی سہولت دیتی ہیں۔ if-else اس کی ایک مثال ہے۔ ہم if-else کو استعمال کرتے ہوئے جب چاہیں پروگرام کے بہاؤ میں حسبِ منشاء تبدیلی کر سکتے ہیں۔ لوپس بھی کنٹرول اسٹرکچر کی طرح کام کرتی ہیں۔ ان کے ذریعے کسی خاص شرط کے پورا ہونے تک کسی مخصوص کوڈ کو بار بار ایگزی کیوٹ کیا جاتا ہے۔ فرض کریں کہ آپ کو فارم پر 100 بار اپنا نام لکھنا ہے۔ اگر آپ ایسا بار بار فارم پر لیبل بنا کر کریں گے تو اس میں بہت زیادہ وقت صرف ہوگا۔ لیکن یہی کام آپ اگر لوپس کے ذریعے کریں تو چند سیکنڈوں میں یہ کام مکمل ہوجائے گا۔

وی بی ڈاٹ نیٹ میں لوپس 6 اقسام کی ہوتی ہیں۔

1- Do Loop, 2- For Next, 3-For Each Next,
4- While End While, 5- With End With,
6-Nested Loop

Do Loop میں پہلے کوڈ چلایا جاتا ہے، پھر کنڈیشن چیک کی جاتی ہے۔ اگر کنڈیشن true ہو تو دوبارہ پہلے والا کوڈ چلایا جاتا ہے۔ اگر کنڈیشن false ہوجائے تو پروگرام لوپ سے نکل کر آگے بڑھ جاتا ہے۔ اسے کیسے استعمال کیا جاتا ہے، اس کے لئے درج ذیل کوڈ ملاحظہ کیجئے:

```
Dim x As Integer = 0
Do
    Console.WriteLine("Value of x is:" & x)
    x = x + 1
Loop While (x < 10)
```

چونکہ لوپ کی اس قسم میں کنڈیشن بعد میں چیک ہوتی ہے، اس لئے کوڈ ایک بار لازمی ایگزی کیوٹ ہوتا ہے۔ جب آپ اوپر دیئے گئے کوڈ کو کسی بٹن کے کلک ایونٹ یا فارم کے لوڈ ایونٹ پر لکھیں گے تو ویژول اسٹوڈیو کی آؤٹ پٹ ونڈو میں آپ کو کچھ ایسا لکھا نظر آئے گا:

```
Value of x is:0
Value of x is:1
Value of x is:2
.....
Value of x is:9
```

اگر آپ کو آؤٹ پٹ ونڈو نظر نہ آرہی ہو تو View مینو میں سے Other Windows اور پھر Output پر کلک کریں۔

For Next لوپ کوڈ کے کسی مخصوص بلاک کو دی گئی تعداد میں چلاتا ہے۔ اگر ہمیں کوئی کام دس بار انجام دینا ہوتو ہم for لوپ کو اس طرح سے استعمال کریں گے:

```
For x = 1 to 10
        Console.WriteLine("Hello")
Next
```

یہاں نوٹ کیجئے کہ ویری ایبل x کی قدر میں for لوپ ہر بار خود ہی ایک کا اضافہ کرتی رہے گی اور یہ ویری ایبل استعمال بھی کیا جاسکتا ہے۔

```
For x = 1 to 10
      Console.WriteLine("Value of X is:" & x)
Next
```

لوپس کی باقی اقسام کا تعارف اور استعمال ہم آئندہ آنے والی قسطوں کے لئے بچا کے رکھتے ہیں۔ فی الحال ہم نے جو کچھ ابھی سیکھا ہے، اس کے ذریعے ایک پروجیکٹ بناتے ہیں۔

ہم ایک ایسا پروگرام بنانا چاہتے ہیں جو کہ دیئے گئے عدد کا ٹیبل (ٹائمز ٹیبل یا ملٹی پلیکیشن ٹیبل) ہمیں فراہم کرے۔ تو آیئے شروع کرتے ہیں۔

پہلے ویژول اسٹوڈیو کھول کر نیا پروجیکٹ بنالیں۔ فارم پر ایک ٹیکسٹ باکس، ایک بٹن اور لیبل شامل کریں۔ ٹیکسٹ باکس کی name پراپرٹی کی ویلیو txtnumber کردیں۔ جبکہ بٹن کا نام txtstart اور لیبل کا نام txttable کردیں۔ بٹن کی Text پراپرٹی کی قدر Show Table کردیں جبکہ لیبل کی Text پراپرٹی کو خالی کردیں۔ آپ تصویر نمبر 1 میں دیکھ سکتے ہیں کہ ہم نے کس طرح ان کنٹرولز کو فارم پر رکھا ہے۔ آپ بھی انہیں ایسے ہی مرتب کریں۔

فارم کی ڈیزائننگ مکمل کرنے کے بعد اب ہم اس کی کوڈنگ کی جانب بڑھتے ہیں۔ بٹن پر ڈبل کلک کرکے کوڈ ونڈو کھول لیں۔ بٹن کے کلک ایونٹ پر ہم یہ کوڈ لکھیں گے:

```
If IsNumeric(txtnumber.Text) Then
    Dim strTable As String
    For x = 1 To 10
        strTable = strTable & txtnumber.Text
         & " x " & x & "=" & txtnumber.Text * x
         & vbNewLine
     Next
    lbltable.Text = strTable
Else
        MsgBox("Please enter a number")
End If
```

اس سے پہلے کہ ہم اس پروگرام کو چلائیں، ہم اس کوڈ کو سمجھنے کی کوشش کرتے ہیں۔ ہم نے سب سے پہلے isNumeric فنکشن کے ذریعے چیک کیا کہ یوزر نے نمبر ہی ٹائپ کیا ہے یا کچھ اور۔ اگر نمبر ٹائپ کیا ہے تو ہم آگے بڑھ جائیں گے جبکہ نمبر نہ ہونے کی صورت میں یوزر کو ایک پیغام نظر آئے گا کہ برائے مہربانی نمبر انٹر کیجئے۔

جب یوزر ٹیکسٹ فیلڈ میں نمبر ٹائپ کرکے Show Table کے بٹن پر کلک کرتا ہے تو isNumeric کی شرط پوری ہوجاتی ہے۔ آگے ہم نے ایک اسٹرنگ ویری ایبل strTable بنایا ہے۔ اس میں ہم ٹیبل بنا کر محفوظ کریں گے اور بعد میں اسے لیبل میں ظاہر کریں گے۔ اس سے آگے آپ For لوپ استعمال کیا گیا ہے جو کہ دس بار چلتا ہے اور ہر بار چلنے پر x کی قدر میں ایک کا اضافہ ہوجاتا ہے۔ اگلی اسٹیٹمنٹ میں آپ بہت سے ویری ایبلز کو ایک دوسرے کے ساتھ concat ہوتا دیکھ سکتے ہیں۔ ہم پہلے ہی آپ کو بتا

چکے ہیں کہ اینڈ کا نشان یعنی & دو اسٹرنگز کو جوڑنے کے لئے استعمال کیا جاتا ہے اور یہ concat آپریٹر کہلاتا ہے۔ آخر میں vbNewLine کا استعمال کیا گیا ہے۔ آپ چاہیں تو اس کی جگہ vbCrlf بھی استعمال کر سکتے ہیں۔ یہ وی بی ڈاٹ نیٹ میں شامل contants میں سے ہیں جنہیں مخصوص کاموں کی انجام دہی کے لئے بنایا گیا ہے۔ یہ اسٹرنگ میں نئی لائن شامل کرنے کے لئے ہے۔ آپ اس کی جگہ یہ اسٹیٹمنٹ چونکہ for لوپ کے اندر ہے اس لئے یہ دس بار چلتی ہے۔ لوپ کے ختم ہوجانے کے بعد ہم نے لیبل کی ٹیکسٹ پراپرٹی کی ویلیو strTable کردی۔ اس طرح strTable میں محفوظ تمام ٹیکسٹ لیبل میں ظاہر ہوگیا۔

اس پروگرام کو چلائیں (تصویر نمبر 2) اور اس میں خامیاں ڈھونڈنے کی کوشش کریں۔ ہمیں جو خامیاں اس میں ملیں، وہ یہ ہیں:

⇦ ٹیبل صرف 1 تا 10 تک ہی بنتا ہے۔ بڑے ٹیبل بنانے کی گنجائش موجود نہیں۔

⇦ ٹیبل بننے کے بعد اسے سلیکٹ یا کاپی نہیں کیا جا سکتا۔

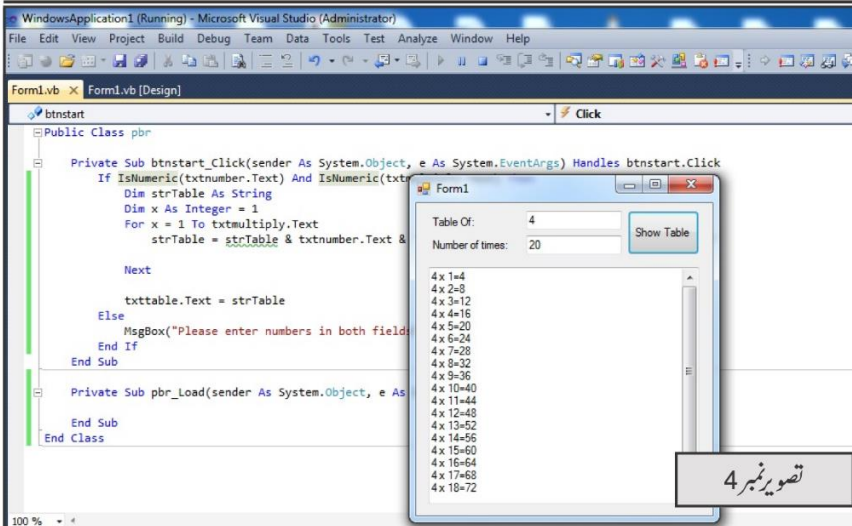
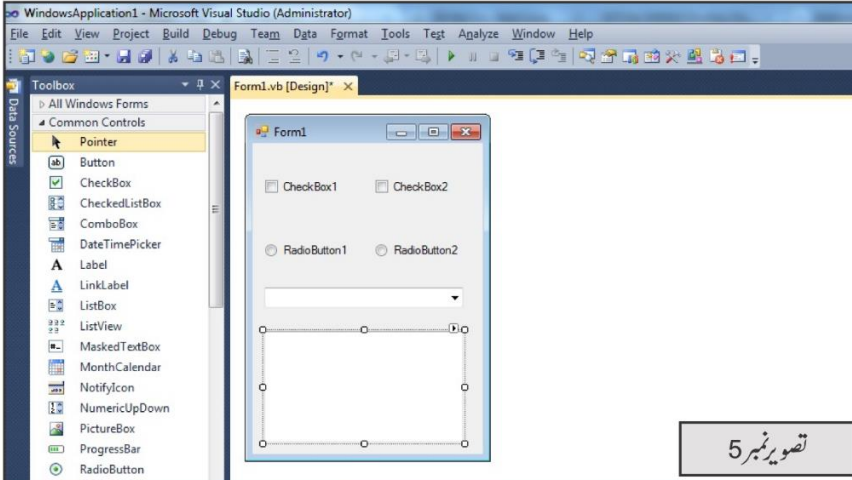
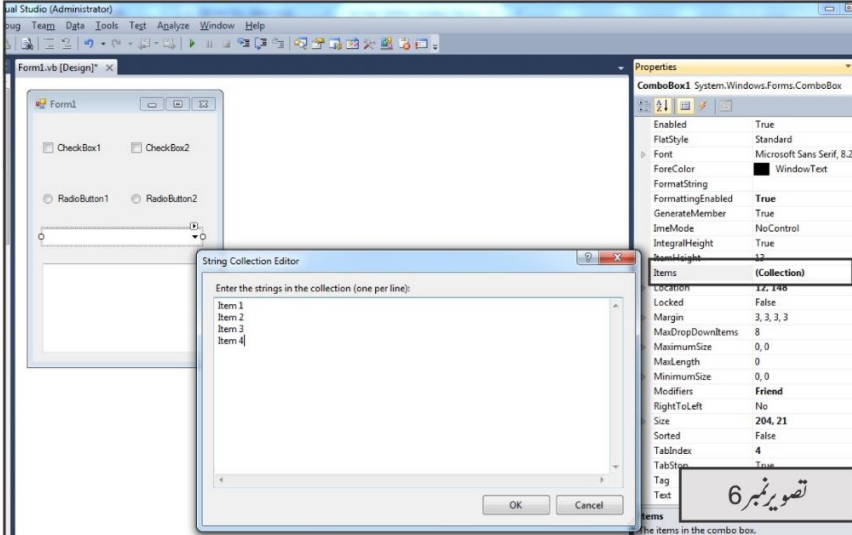
پہلے شکایت کو دور کرنے کے لئے ہم فارم پر مزید ایک ٹیکسٹ باکس شامل کریں گے اور اسے txtmultiply کا نام دیں گے۔ جبکہ دوسرا مسئلہ دور کرنے کے لئے لیبل کو ڈیلیٹ کریں اور اس کی جگہ ایک اور ٹیکسٹ فیلڈ شامل کردیں۔ اس ٹیکسٹ باکس کی پراپرٹیز میں یہ تبدیلیاں کیجئے:

Name: txttable

Multiline: True

Scrollbars: Verticle

پروگرام کو مزید بہتر بنانے کے لئے ہم نے اس میں کچھ لیبلز کا اضافہ بھی کیا ہے اور کنٹرولز کی پوزیشن بھی تبدیل کی ہے۔ اسے آپ تصویر نمبر 3 میں دیکھ سکتے ہیں۔ اب فارم پر موجود واحد بٹن پر ڈبل کلک کرکے اس کے کلک ایونٹ میں موجود کوڈ کچھ تبدیل کریں:

```
If IsNumeric(txtnumber.Text)
    And IsNumeric(txtmultiply.Text) Then
Dim strTable As String
Dim x As Integer = 1
For x = 1 To txtmultiply.Text
strTable = strTable & txtnumber.Text &
 " x " & x & "=" & txtnumber.Text * x &
vbCrLf
```

تصویر نمبر 4

تصویر نمبر 5

تصویر نمبر 6

```
Next
txttable.Text = strTable
Else
MsgBox("Please enter numbers in both fields")
End If
```

اس کوڈ میں کوئی نئی چیز استعمال نہیں۔ البتہ ہم نے نئے کنٹرولز کو مدنظر رکھتے ہوئے کوڈ لکھا ہے۔ اس پروگرام کو ایگزی کیوٹ کرنے پر آپ دیکھیں گے کہ اب کی بار یہ بہت بہتر کام کررہا ہے اور آپ ٹیکسٹ باکس سے ٹیبل کو کاپی بھی کرسکتے ہیں۔

ابھی تک ہم نے صرف چند ہی کنٹرولز استعمال کئے ہیں۔ اب ہم چند مزید کنٹرولز کے بارے میں پڑھیں گے۔ یہ کنٹرولز ریڈیو بٹن، چیک باکس اور لسٹ ہیں۔ ان کا کام کرنے کا طریقہ کار ہم ایک چھوٹا سا پروجیکٹ بنا کرسیکھیں گے۔

نیا پروجیکٹ کھول کر فارم پر 2 ریڈیو بٹنز، 2 چیک باکس، ایک Combo Box اور ٹیکسٹ باکس شامل کردیں۔ آپ تصویر نمبر 5 میں دیکھ سکتے ہیں کہ ہم نے کیسے ان کنٹرولز کو فارم پر ترتیب دیا ہے۔ ان کے نام آپ جو چاہیں رکھ لیں۔ البتہ ان کی کچھ پراپرٹیز کو حسب ذیل انداز میں تبدیل کردیں:

Checkbox1

Value: CheckBox 1

Checkbox2

Value: CheckBox 2

RadioButton1

Value: RadioButton 1

```
TextBox1.Text = TextBox1.Text &
TimeOfDay.ToString & " : CheckBox 2 is
Checked" & vbNewLine
Else
TextBox1.Text = TextBox1.Text &
TimeOfDay.ToString & " : CheckBox 2 is
UnChecked" & vbNewLine
End If
End Sub
Private Sub
RadioButton1_CheckedChanged(sender As
System.Object, e As System.EventArgs) Handles
RadioButton1.CheckedChanged
If RadioButton1.Checked Then
TextBox1.Text = TextBox1.Text &
TimeOfDay.ToString & " : RadioButton 1 is
Checked" & vbNewLine
Else
TextBox1.Text = TextBox1.Text &
TimeOfDay.ToString & " : RadioButton 1 is
UnChecked" & vbNewLine
End If
End Sub
Private Sub
RadioButton2_CheckedChanged(sender As
Object, e As System.EventArgs) Handles
RadioButton2.CheckedChanged
If RadioButton2.Checked Then
TextBox1.Text = TextBox1.Text &
TimeOfDay.ToString & " : RadioButton 2 is
Checked" & vbNewLine
Else
```

RadioButton2

Value: RadioButton 2

ComboBox1

Items: "Item 1" "Item 2" "Item 3"

TextBox1

Multiline: True

اب آپ پہلے چیک باکس پر ڈبل کلک کریں جس سے کوڈ ونڈو کھل جائے گی۔آپ دیکھیں گے کہ CheckedChanged ایونٹ کے لئے پہلے ہی ہینڈلر فنکشن شروع کردیا گیا ہے۔یہ ایونٹ اس فائر یا ٹرگر ہوتا ہے جب چیک باکس کی حالت میں کوئی تبدیلی آتی ہے۔یعنی اگر وہ چیک تھا تو ان چیک کرنے سے یہ ایونٹ فائر ہوجائے گا۔

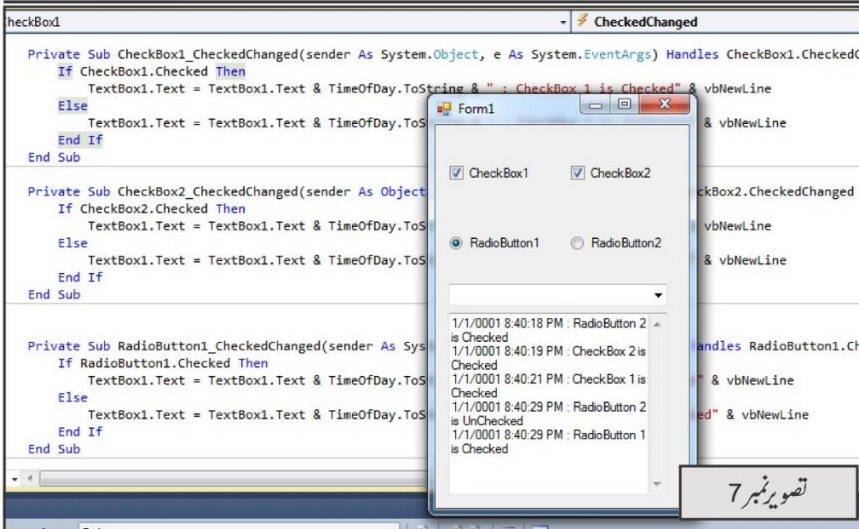
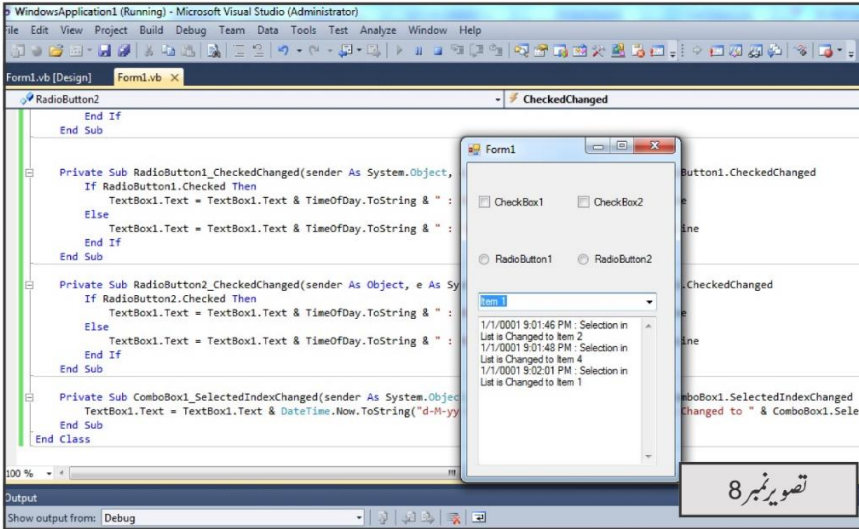
اس ایونٹ ہینڈلر میں آپ یہ تحریر کریں:

```
If CheckBox1.Checked Then
TextBox1.Text = TextBox1.Text &
TimeOfDay.ToString & " : CheckBox 1
is Checked" & vbNewLine
Else
TextBox1.Text = TextBox1.Text &
TimeOfDay.ToString & " : CheckBox 1 is
UnChecked" & vbNewLine
End If
```

اس کوڈ میں TimeOfDay ایک نئی چیز ہے۔یہ ہم نے بلاوجہ شامل کی ہے تاکہ آپ کو ایک نئی چیز سیکھنے کو مل جائے۔اس آبجیکٹ کے ذریعے آپ موجودہ وقت حاصل کرسکتے ہیں۔

ہم نے اس کوڈ کے ذریعے پہلے چیک کیا کہ کیا چیک باکس کو check کیا گیا ہے؟ ہاں یا ناں کے مطابق ہم نے ایک لائن ٹیکسٹ باکس میں شامل کردی۔

باقی کے چیک باکسز اور ریڈیو بٹن کے لئے کوڈ یہ ہوگا:

```
Private Sub
CheckBox2_CheckedChanged(sender As Object,
e As System.EventArgs) Handles
CheckBox2.CheckedChanged
If CheckBox2.Checked Then
```

تصویر نمبر 7

تصویر نمبر 8

```
TextBox1.Text =
TextBox1.Text &
TimeOfDay.ToString & " :
RadioButton 2 is
UnChecked" &
vbNewLine
End If
End Sub
```

اب اس سے پہلے کہ ہم کومبولسٹ کے لئے کوڈ لکھیں، آیئے اپنے بنائے پروگرام کو چلا کر دیکھتے ہیں۔ کی بورڈ سے F5 کا بٹن دبا کر ڈی بگنگ شروع کیجئے۔ پروگرام جب لوڈ ہوجائے تو پہلے چیک باکس پر کلک کیجئے۔ آپ دیکھیں گے کہ نیچے موجود ٹیکسٹ باکس میں ٹیکسٹ کا اضافہ ہوگیا ہے۔ آپ دوسرے چیک باکس کو بھی چیک کردیں۔ یہی عمل ریڈیو بٹن کے ساتھ بھی کریں۔ لیکن آپ دیکھیں گے کہ آپ بیک وقت دونوں ریڈیو بٹنز کو سلیکٹ نہیں کرسکتے۔ تاہم چیک باکس کے لئے ایسی کوئی پابندی نہیں۔

کیا آپ نے نوٹ کیا کہ ریڈیو بٹن اور چیک باکس کے اسٹیٹس میں تبدیلی سے ٹیکسٹ باکس میں جو ٹیکسٹ ظاہر ہورہا ہے اس کے شروع میں وقت تو ٹھیک ہے لیکن تاریخ غلط ہے؟

جی ہاں، یہ بھی ہم نے جان بوجھ کر کیا ہے کہ آپ کو ایک نئے آبجیکٹ کے بارے میں جو بتانا تھا۔ ہم نے TimeOfDay کا آبجیکٹ استعمال کیا تھا جو بذات خود DateTime آبجیکٹ کی ایک پراپرٹی ہے۔ خیر، آپ TimeOfDay کو درج ذیل کوڈ سے بدل دیں:

```
DateTime.Now.ToString("d-M-yy HH:mm")
```

اس بار پروگرام چلانے پر بالکل درست تاریخ اور وقت بتائے گا۔ تاریخ اور وقت کے بارے میں مزید باتیں ہم انشاءاللہ اگلی اقساط میں جانیں گے۔

فی الحال ہم اپنی توجہ ایک بار پھر پروجیکٹ کی جانب مرکوز کرتے ہوئے کومبو لسٹ کے لئے کوڈ لکھتے ہیں۔

آپ ڈیزائن موڈ میں آکر کومبولسٹ پر ڈبل کلک کریں۔ اس کا ڈیفالٹ ایونٹ ہینڈلر SelectedIndexChanged ہے۔ یعنی جیسے ہی لسٹ میں موجود کوئی نیا آئٹم منتخب کیا جائے، یہ ایونٹ فائر/ٹرگر ہوجائے گا۔ اس کے ایونٹ ہینڈلر فنکشن میں آپ یہ کوڈ لکھیں:

```
TextBox1.Text = TextBox1.Text &
DateTime.Now.ToString("d-M-yy HH:mm") & " :
RadioButton 2 is Checked" & vbNewLine
```

اب بغیر کسی انتظار کے فوراً اس پروگرام کو ایگزیکیوٹ کیجئے اور تمام کنٹرولز کے کام کرنے کے طریقہ کار کو جانچیں۔

علمدار حسین

ورڈپریس ویب سائٹ کو ہیکنگ سے محفوظ بنائیں

دنیائے ویب میں موجود بائیس فیصد فعال ڈومینز ''ورڈ پریس'' استعمال کر رہے ہیں۔ یعنی قریباً ہر چار میں سے ایک ویب سائٹ ورڈ پریس پر بنائی گئی ہے۔ اپنی لچکدار ساخت اور استعمال میں آسانی کی وجہ سے بلاشبہ ورڈ پریس اس وقت دنیا کا معروف ترین کانٹینٹ منیجمنٹ سسٹم (CSM) ہے۔ ایک وقت تھا جب ویب سائٹ بنانا جان جوکھوں کا کام ہوا کرتا تھا، اب تو ورڈ پریس کے ذریعے چند منٹوں میں کوئی بھی اپنی ویب سائٹ بنا سکتا ہے۔ جو چیز اس قدر مشہور ہو اور اتنی بڑی تعداد میں استعمال ہو رہی ہو ہیکرز کا نشانہ نہ بنے یہ ممکن نہیں۔ اس وقت ورڈ پریس ہیکرز کا سب سے بڑا نشانہ ہے۔ آئے دن ورڈ پریس کی سیکڑوں ویب سائٹس ہیک ہو رہی ہیں۔ اس ہیکنگ کی وجہ ورڈ پریس میں موجود اس کی اپنی کوئی خامی کے علاوہ انسٹال کسی پلگ اِن میں کوئی خرابی بھی ہوسکتی ہے۔ سب سے بڑھ کر ویب ڈیویلپر یا ایڈمن کی اپنی کسی غلطی کی بنا پر بھی ورڈ پریس پر بنائی گئی ویب سائٹ باآسانی ہیک ہوسکتی ہے۔

اگر آپ ورڈ پریس کو اچھی طرح جانتے ہیں یا آپ ایک اچھے ویب ڈیویلپر ہیں جسے بہت اچھی کوڈنگ آتی ہے تو اس کا یہ مطلب نہیں کہ آپ ورڈ پریس کو ہیکنگ سے بچا سکتے ہیں۔ ورڈ پریس ویب سائٹ کو محفوظ رکھنے کے لیے کئی ایک چیزوں کا پتا ہونا چاہیے۔ آئیے آپ کو کچھ ایسی ہی سیکیوریٹی ٹپس کے بارے میں بتاتے ہیں۔

ویب سائٹس کون ہیک کرتے ہیں؟

ویب سائٹس کا خراب اور ہیک ہونا بہت ہی عام سی بات ہے۔ میں خود سیکڑوں ہیک شدہ اور وائرس زدہ ویب سائٹس ٹھیک کر چکا ہوں۔ ویب سائٹ کو واپس اصلی حالت میں لانے کے بعد صاحب ویب سائٹ کا ہمیشہ مجھ سے یہی سوال ہوتا ہے کہ ''میں اپنی ویب سائٹ کو ہیکرز سے کیسے محفوظ بنا سکتا ہوں؟''

اور میرا جواب ہمیشہ یہی ہوتا ہے کہ ''ہیکرز آپ کی ویب سائٹ کے پیچھے نہیں پڑے ہوئے، بلکہ یہ بوٹس اور اسکرپٹ ہیں جو یہ کام انجام دے رہے ہیں۔''

سن 2012 میں لگ بھگ ایک بلین ہیکنگ کی کوششیں کی گئیں۔ آپ خود سوچیں کہ دنیا میں اتنے ہیکرز موجود ہیں جو اتنی بڑی تعداد میں کوششیں کر سکتے ہیں؟ اگر دنیا بھر کے ہیکرز ہفتے کے ساتوں دن چوبیس گھنٹے بھی ہیکنگ کی کوششیں کرتے رہیں تو اس نمبر کو پہنچنا بہت مشکل ہے۔ البتہ بلاشبہ دنیا میں اتنے اسکرپٹس اور بوٹس ضرور موجود ہیں جو دن رات اپنے کام میں مگن رہتے ہیں۔ ہیکرز اسکرپٹس بناتے ہیں اور بوٹس انھیں خودکار طریقے سے ویب سائٹس پر آزماتے رہتے ہیں۔ زیادہ تر ایسے اسکرپٹس وائرس زدہ کمپیوٹرز سے پھیلتے ہیں۔ کمپیوٹرز جن پر ٹروجن، مال ویئر، اسپائی ویئر وغیرہ حملہ آور ہوتے ہیں وہ ایسے اسکرپٹس کو پھیلانے کا خودکار کام شروع کر دیتے ہیں۔ زیادہ تر روس اور چین سے تعلق رکھنے والے ہیکرز یہ اسکرپٹس بناتے ہیں۔ البتہ عرب ہیکرز بھی کسی سے پیچھے نہیں خاص کر ترکی اور انڈونیشیا سے تعلق رکھنے والے ہیکرز بھی خوب ورڈ پریس کو نشانہ بنائے ہوئے ہیں۔

آخر ہیکرز آپ کی ویب سائٹ سے کیا چاہتے ہیں؟

ہیک ہونے والی ویب سائٹ کے مالک کا اگلا سوال یہ ہوتا ہے کہ ''آخر ہیکرز نے میری ہی ویب سائٹ کو کیوں نشانہ بنایا؟ میری ویب سائٹ سے وہ کیا

حاصل کرنا چاہتے ہیں؟''

ایک وقت تھا جب کسی خاص مقصد یا پیغام کے لیے کوئی ویب سائٹ ہیک کی جاتی تھی۔ آج کل کے ''اسکرپٹ کڈی'' بنا کسی امتیاز کے جو کمزور ورڈپریس یا کوئی دوسری ویب سائٹ ملے ہیک کرنے کی کوشش میں لگ جاتے ہیں۔ زیادہ تر ہیک شدہ ویب سائٹس کو ٹھیک کرتے ہوئے بندہ سوچتا ہے کہ اسے ہیک کہنا بھی درست نہیں۔ کیونکہ ہمیں پتا ہوتا ہے کہ ورڈپریس کی کن فائلوں میں تبدیلی کی گئی ہوگی۔ اس لیے براہ راست چند فائلوں کو دیکھ کر ویب سائٹ ٹھیک کی جا سکتی ہے۔ اسکرپٹس کے ذریعے کی گئی اس ہیکنگ کا زیادہ تر مقصد ری ڈائریکشن ہوتی ہے۔ تاکہ آپ کی ویب سائٹ پر آنے والا ٹریفک ان کی ویب سائٹ کی طرف موڑا جا سکے۔ ظاہر ہے ایسی ویب سائٹس زیادہ تر منشیات، جوئے اور غیر اخلاقی مواد کے حوالے سے ہوتی ہیں۔

کوئی بھی اپنی ورڈپریس ویب سائٹ کو محفوظ بنا سکتا ہے

جس طرح کہتے ہیں کہ احتیاط علاج سے بہتر ہے بالکل اسی طرح ویب سائٹ ہیک ہونے کے بعد سکیوریٹی تراکیب جاننے سے بہتر ہے کہ آپ پہلے ہی ان کے بارے میں واقف ہوں۔ ایک ورڈپریس ویب سائٹ کی سکیوریٹی بڑھانا کوئی ایسا مشکل کام نہیں ہے۔ اس کام کے لیے آپ کا ویب ڈیویلپر ہونا بھی ضروری نہیں۔ بہت ہی آسانی کے ساتھ چند ٹپس استعمال کرتے ہوئے آپ اپنی ورڈپریس ویب سائٹ کو ہیکنگ پروف نہ سہی کم از کم کافی حد تک محفوظ ضرور بنا سکتے ہیں۔ آیئے آپ کو ان ٹپس کے بارے میں بتاتے ہیں۔

ایڈمن یوزر نیم اور پاس ورڈ

ورڈپریس انسٹالیشن کے دوران ایڈمن یوزر نیم فراہم کرتا ہے۔ یوزر نیم ایڈمن استعمال کرنے کا مطلب ہے کہ کم از کم ہیکرز کو ایک تصدیقی کنجی آپ نے فراہم کر دی ہے جسے استعمال کرتے ہوئے وہ ویب سائٹ میں داخل ہونے کی کوشش کر سکتا ہے۔ اس سے بچنے کے لیے ورڈپریس کی انسٹالیشن کے فوراً بعد اس یوزر نیم کو بدل کر کچھ اور کر لیں۔

فرض کریں آپ ایک اے ٹی ایم سے پیسے نکال رہے ہوں اور کوئی شخص آپ کے پیچھے کھڑا آپ کا پن نمبر دیکھ رہا ہو تو یقیناً آپ کو تشویش ہو جائے گی۔ اسی طرح اپنی ورڈپریس ویب سائٹ کا ایڈمن پینل لاگ اِن کرتے ہوئے آپ کو احتیاط سے کام لینا چاہیے۔ ہمیشہ یہی سوچیں کہ کوئی نہ کوئی آپ کے پاس ورڈ کی تاک میں ہے۔

اپنے گھر پر وائی فائی نیٹ ورک استعمال کرتے ہوئے یقیناً آپ کے وائی فائی کنکشن پر پاس ورڈ اور کچھ اِنکرپشن ضرور ہوتی، لیکن پبلک وائی فائی استعمال کرتے ہوئے کبھی بھی اپنا ورڈپریس ایڈمن یا ایف ٹی پی سرور مت کنیکٹ کریں۔ بعض اوقات یہ کنکشن محفوظ نہیں ہوتا۔ پبلک وائی فائی پر اپنی ویب سائٹ لاگ اِن کرتے ہوئے ہمیشہ ان باتوں کا خیال رکھیں:

ورڈپریس ایڈمن پینل مت لاگ اِن کریں ماسوائے اس کے کہ آپ ''ون ٹائم پاس ورڈ'' استعمال کر رہے ہوں۔

ایف ٹی پی کی بجائے ایس ایف ٹی پی استعمال کریں جو کہ محفوظ ہوتا ہے۔

ہوسٹنگ کنٹرول پینل کھولنے کے لیے ہمیشہ https پروٹوکول استعمال کریں۔

گھر یا اپنے محفوظ نیٹ ورک پر واپس آنے کے بعد فوراً اپنے پاس ورڈز ضرور بدل لیں۔ ہمیشہ مشکل پاس ورڈ استعمال کریں جسے توڑنا بہت ہی مشکل ہو۔

ڈیٹابیس ٹیبل پری فکس بدلیں

ورڈپریس انسٹال ہوتے ہوئے ہمیشہ ایک جیسا Prefix استعمال کرتا ہے۔ یعنی اگر آپ ورڈپریس کی انسٹالیشن کے دوران پری فکس نہ بدلیں تو ڈیٹابیس ٹیبل ضرور wp کے نام سے شروع ہوتی ہے۔ ہیکرز ورڈپریس کے ڈیٹابیس کو بھی نشانہ بناتے ہیں اور اس پر ایس کیو ایل انجکشن کے ذریعے حملہ کرتے ہیں۔ اگر آپ ورڈپریس انسٹال کرتے وقت ڈیٹابیس ٹیبل پری فکس کو بدل دیں تو یہ ایس

Hostname	localhost
Username	
Password	
Database Name	
Table Prefix	wp_

کیو ایل انجکشن کا خطرہ انتہائی کم ہو جاتا ہے۔

ورڈپریس ایڈمن پینل سے تھیم ایڈیٹنگ بند کریں

ورڈپریس کے ایڈمن پینل سے نہ صرف مواد اپنی ویب سائٹ پر شائع کیا جا سکتا ہے بلکہ تھیم اور پلگ اِنز کی فائلز کو بھی براہِ راست ایڈیٹ کیا جا سکتا ہے۔ اگرچہ یہ ویب سائٹ میں تبدیلیاں کرنے کا بہت سہل طریقہ کار ہے لیکن یہ

انتہائی خطرناک بات بھی ہے۔ اگر ہیکر کسی طرح آپ کے ایڈمن پینل میں داخل ہونے کے قابل ہوگیا تو وہ باآسانی ویب سائٹ ہیک کرسکتا ہے۔ آپ کا پاس ورڈ چوری ہوجاتا ہے، ہیک ہوجاتا ہے، یا ڈیٹا بیس تک رسائی حاصل کرکے ہیکر ایڈمن یوزر بنالیتا ہے تو ویب سائٹ کا کوئی بھی صفحہ اس کی دسترس سے محفوظ نہیں رہے گا۔ اس لیے بہتر یہی ہے کہ ورڈپریس ایڈمن پینل میں دستیاب یہ ایڈیٹنگ کے حقوق ختم کردیے جائیں۔ یہ کام انتہائی آسان ہے، اس کے لیے آپ کو wp-config فائل میں صرف ایک درج ذیل لائن کا اضافہ کرنا ہوگا:

```
#DISABLE EDITING IN ADMIN PANEL
define('DISALLOW_FILE_EDIT', true);
```

wp-adminڈائریکٹری پر پاس ورڈ لگائیں

ڈبلیو پی ایڈمن ڈائریکٹری آپ کے ورڈپریس ایڈمن پینل میں جانے کا راستہ ہے۔ اپنی ورڈپریس ویب سائٹ پر سکیوریٹی کی ایک اضافی تہہ بنانے کے لیے آپ اس ڈائریکٹری پر پاس ورڈ لگا سکتے ہیں۔ اس طرح بطور ایڈمن لاگ اِن ہونے سے پہلے ڈائریکٹری کا لاگ اِن پاس ورڈ فراہم کرنا ہوگا۔ اگر آپ سی پینل استعمال کررہے ہیں تو باآسانی اس ڈائریکٹری پر پاس ورڈ لگا سکتے ہیں۔ اس کے لیے ویب ہوسٹنگ کنٹرول پینل سے "Password Protect Directories" کے آپشن پر کلک کرکے wp-admin کی ڈائریکٹری منتخب کرکے اس پر پاس ورڈ سیٹ کردیں۔ اب اس ڈائریکٹری تک رسائی حاصل کرنے کے لیے ضروری ہوگا کہ پہلے یہ یوزرنیم پاس ورڈ فراہم کیا جائے۔ ایڈمن یوزرنیم تبدیل کرنے کے بعد اور ایڈمن ڈائریکٹری پر پاس ورڈ لگانے کے بعد سمجھیں آپ نے بروٹ فورس اٹیک کا راستہ بند کردیا ہے۔

کونٹینٹ ڈائریکٹری کا نام بدلیں

جیسا کہ ہم نے ذکر کیا کہ انٹرنیٹ پر بوٹس مصروف ہوتے ہیں، انھیں جو کام دیا جاتا ہے یہ صرف وہی کرتے رہتے ہیں۔ چونکہ سبھی کو پتا ہوتا ہے کہ ورڈپریس کے پلگ اِنز اور تھیمز کس ربط پر موجود ہوتے ہیں اس لیے بوٹس سیدھا اس ربط پر جاکر کسی پلگ اِن یا ورڈپریس کے ڈیفالٹ تھیمز میں موجود خرابی کو تلاش کرتے ہیں۔ اگر کونٹینٹ ڈائریکٹری کا نام بدل دیا جائے تو یہ بوٹس اپنے کام میں ناکام ہوجاتے ہیں۔ یہی طریقہ استعمال کرتے ہوئے ہیکرز نے timthumb نامی ایک پلگ اِن میں موجود خامی کو استعمال کرتے ہوئے لاکھوں ویب سائٹس کو ہیک کیا تھا۔

کونٹینٹ ڈائریکٹری کا نام ورڈپریس ویب سائٹ بناتے ہوئے بدلا جاتا ہے۔ اگر آپ ایک چلتی ہوئی ورڈپریس ویب سائٹ پر یہ عمل کریں گے تو ویب سائٹ خراب ہوسکتی ہے۔ کم از کم سست ہیکرز اور بوٹس وغیرہ سے یہ ڈائریکٹری چھپ جانے سے ویب سائٹ کی سکیوریٹی میں کافی اضافہ ہوجاتا ہے۔

اپنی ویب سائٹ اسکین کریں

اپنی ویب سائٹ کو وائرس یا مال ویئر کے لیے اسکین کرنے میں کوئی حرج کی بات نہیں۔ آن لائن کئی مفت اسکینرز دستیاب ہیں جیسے کہ سوکوری اور کوٹیرا اسکینر۔

http://sitecheck.sucuri.net

http://quttera.com

یہ دونوں بہترین اسکینر ہیں خاص کر سوکوری کی کارکردگی بہت لاجواب ہے۔ اگر ویب سائٹ مال ویئر زدہ ہوئی تو یہ اسکینر آپ کو مال ویئر ڈمپ تک فراہم کر دیتی ہے۔ اس کے علاوہ یہ بھی بتایا جاتا ہے کہ ویب سائٹ کسی سرچ انجن میں بلیک لسٹڈ تو نہیں ہوچکی۔ اچھی بات یہ ہے کہ دونوں ویب سائٹس کے ورڈ پریس پلگ اِنز بھی دستیاب ہیں۔ جن کو اپنی ویب سائٹ میں شامل کر کے آپ اپنی ویب سائٹ کی سکیوریٹی خامیوں پر نظر رکھ سکتے ہیں۔ پلگ اِن انسٹال کر کے ویب سائٹ کی اسکیننگ زیادہ اچھے نتائج فراہم کرتی ہے۔

سوکوری اسکینر ورڈ پریس پلگ اِن درج ذیل ربط ملاحظہ فرمائیں:

wordpress.org/plugins/sucuri-scanner

چوری شدہ تھیم

ورڈ پریس ویب سائٹس کے ہیک اور وائرس سے متاثر ہونے کی ایک بڑی وجہ چوری شدہ تھیم کا استعمال ہے۔ پریمیئم تھیمز چونکہ بہت خوبصورت اور کارکردگی میں بہتر ہوتے ہیں اس لیے لوگ ان کو ترجیح دیتے ہیں لیکن انھیں خریدے بنا۔ کریکس فراہم کرنے والی ویب سائٹس سے ان تھیمز کے کریکڈ یا نلڈ (Nulled) ورژن ڈاؤن لوڈ کر کے اپنی ویب سائٹ پر لگا لیتے ہیں۔

ایسے تھیم فراہم کرنے والے لوگ اکثر ان میں مال ویئر کوڈز شامل کر دیتے ہیں۔ پچاس ساٹھ ڈالر کا تھیم مفت ہاتھ لگ جانے پر لوگ خوشی خوشی انھیں استعمال کرنا شروع کر دیتے ہیں اور چند دن بعد ویب سائٹ کے ہیک ہونے کی صورت میں اس کی ادائیگی کرنا پڑتی ہے۔

اگر آپ قیمتاً دستیاب تھیم خرید نہیں سکتے تو بہتر یہی ہے کہ کوئی مفت تھیم منتخب کر لیں۔ ورڈ پریس کے لیے سیکڑوں بہترین تھیمز بالکل مفت دستیاب ہیں۔ جنھیں آپ اپنی پسند کے مطابق کسٹمائز بھی کر سکتے ہیں۔

اگرچہ ہم کریک یا نلڈ چیزوں کو استعمال کرنے کا کبھی مشورہ نہیں دیتے لیکن اگر آپ کے پاس کوئی ایسا تھیم موجود ہے تو پہلے اسے وائرس ٹوٹل سے ضرور اسکین کر لیں۔

اِن پسند نہ آئے تو اسے غیر فعال کر کے اَن انسٹال کر دیں اور کوئی دوسرا پلگ اِن آزمائیں۔ ایک سے زائد پلگ اِنز کا ایک ساتھ استعمال کوئی اچھا تجربہ ثابت نہیں ہوتا۔

اس کے علاوہ ان پلگ اِنز میں موجود اکثر فیچرز آپ کو سمجھ نہیں آئیں گے کہ ان کا کیا مقصد ہے۔ اور انھیں آزمانے کی صورت میں آپ ویب سائٹ میں گڑبڑ بھی کر سکتے ہیں۔ اگر کچھ ایسا ہو جائے تو گھبرانے کی ضرورت نہیں، اس پلگ اِن کو اپنے FTP سے ڈیلیٹ کر کے دوبارہ کوشش کریں۔

ایسے پلگ اِنز زیادہ تر پہلے مشورہ دیتے ہیں کہ اپنی ویب سائٹ بمعہ ڈیٹا بیس کا بیک اپ بنالیں، تاکہ کسی خرابی کی صورت میں اسے ری اسٹور کر سکیں۔ یہ واقعی اچھا اور قابل عمل مشورہ ہے۔

ہر سکیوریٹی پلگ اِن کے کام کرنے کا اپنا الگ طریقہ کار ہوتا ہے۔ اگر مشہور اور بہترین پلگ اِنز کی بات کی جائے تو ہم آپ کو بُلٹ پروف سکیوریٹی، ورڈ فینس سکیوریٹی اور آئی تھیمز سکیوریٹی (بیٹر ڈبلیو پی سکیوریٹی) پلگ اِنز کا مشورہ دیں گے۔

wordpress.org/extend/plugins/bulletproof-security

wordpress.org/extend/plugins/wordfence

wordpress.org/extend/plugins/better-wp-security

یہ تمام پلگ اِنز لاکھوں کی تعداد میں ڈاؤن لوڈ ہو چکے ہیں اور ایک بڑی تعداد میں استعمال ہو رہے ہیں۔ یہ پلگ اِنز واقعی بہترین ہیں۔ اگر ورڈ فینس کی بات کی جائے تو یہ چند لمحوں میں آپ کی مکمل ویب سائٹ کو اسکین کر کے رپورٹ فراہم کرتا ہے۔ اس کی اسکیننگ رپورٹ کو بہت ہی تحمل کے ساتھ دیکھیں کیونکہ یہ ہر مشکوک فائل کو آپ کے سامنے پیش کر دیتا ہے جسے یہیں سے ڈیلیٹ کیا جا سکتا ہے اور ڈیلیٹ کی گئی یہ فائل واپس نہیں ملتی۔ اس لیے یہ جس فائل میں مال ویئر کی نشاندہی کرے اسے وائرس ٹوٹل پر اپ لوڈ کر کے پہلے سو فیصد یقین کر لیں کہ وہ واقعی مال ویئر زدہ ہے۔

www.virustotal.com

ورڈ پریس سکیوریٹی پلگ اِنز

ورڈ پریس کے لیے کئی ''آل اِن وَن'' سکیوریٹی پلگ اِنز مفت دستیاب ہے۔ ان میں سے زیادہ تر انسٹال اور کنفیگر کرنے میں بہت آسان ہوتے ہیں اور ان میں درجنوں آپشنز دستیاب ہوتے ہیں۔ اگر آپ کوئی سکیوریٹی پلگ اِن استعمال کرنے کا فیصلہ کریں تو صرف ایک پلگ اِن انسٹال کریں۔ اگر آپ کو یہ پلگ

آئی تھیمز سکیوریٹی (بیٹر ڈبلیو پی سکیوریٹی)

آئی تھیمز سکیوریٹی پلگ اِن میری پہلی ترجیح ہوتی ہے۔ میں ہمیشہ سب کو اسی پلگ اِن کو انسٹال کرنے کا مشورہ دیتا ہوں۔ یہ پلگ اِن بھی نمبر ون ورڈ پریس سکیوریٹی پلگ اِن ہونے کا دعویٰ کرتا ہے۔ اگر اس کی کارکردگی اور ڈاؤن لوڈ ہونے کے اعداد دیکھے جائیں تو یہ سچ بھی لگتا ہے۔ گزشتہ کئی سالوں سے میں

سیکڑوں کلائنٹس کو یہ پلگ اِن انسٹال کر کے دے چکا ہوں اور ہمیشہ اسے کار آمد ہی پایا ہے۔ آئی تھیمز سکیور یٹی پہلے بیٹر ڈبلیو پی سکیوریٹی کے نام سے موجود تھا جس کا نام اب بدل دیا گیا ہے۔

اس پلگ اِن کو واقعی ''آل ان ون'' سکیوریٹی پلگ اِن کہا جا سکتا ہے۔ اس کے فیچرز کی ایک طویل لسٹ ہے۔ اس کے چند خاص خاص فیچرز درج ذیل ہیں:

بیک اپ

یہ پلگ اِن ویب سائٹ کا مکمل بیک اپ بنا کر آپ کو بھیج سکتا ہے۔

لاگ اِنگ (Logging)

404 ایررز، غلط لاگ اِن کوششیں، آپ کی اجازت کے بغیر فائلوں میں ہونے والی تبدیلی اور اس طرح کی کئی چیزیں یہ اپنے پاس نوٹ کر لیتا ہے۔ اس طرح آپ فوراً جان سکتے ہیں کہ کوئی ویب سائٹ کے ساتھ چھیڑ چھاڑ کی کوشش کر رہا ہے۔

فٹ پرنٹس

ورڈ پریس اکثر اس وجہ سے نشانہ بنتا ہے کہ ویب سائٹ کے سورس کوڈ سے پتا چلایا جا سکتا ہے کہ ورڈ پریس کا کون سا ورژن استعمال کیا جا رہا ہے۔ یہ پلگ اِن ورژن کی معلومات اور تھیم کی کوڈنگ سے ظاہر ہونے والی معلومات کو غائب کر دیتا ہے۔

ایڈمن یوزر نیم کی تبدیلی

ورڈ پریس عام انسٹالیشن کے دوران ایڈمنسٹریٹر یوزر جس کے پاس ورڈ پریس منیجمنٹ کے تمام حقوق موجود ہوتے ہیں، admin یوزر نیم متعین کرتا ہے۔ اسے اسی طرح چھوڑ دینا سکیوریٹی کے نظریئے سے ایک غلطی ہے۔ لہٰذا اسے فوراً تبدیل کر دینا چاہیے۔ اس کام کی سہولت بھی اس پلگ اِن میں موجود ہے۔

کونٹینٹ ڈائریکٹری کو ری نیم کرنا

جیسا کہ ہم نے ذکر کیا wp-content ڈائریکٹری کے نام کی تبدیلی ویب سائٹ کو کافی محفوظ بنا دیتی ہے۔ یہ کام بھی اسی پلگ ان سے کیا جا سکتا ہے۔

اپ ڈیٹس نوٹی فیکیشنز کا خاتمہ

ورڈ پریس اور اس کے پلگ اِنز کی اپ ڈیٹس آئے دن ریلیز ہوتی رہتی ہیں۔ یہ پلگ اِن تمام اپ ڈیٹس کی نوٹی فیکیشنز کو غیر فعال کر دیتا ہے۔ اس طرح کوئی نہیں جان سکتا کہ آپ کوئی آؤٹ ڈیٹڈ پلگ اِن استعمال کر رہے ہیں۔

حملے کی اطلاع اور حفاظت

اس پلگ اِن کی موجودگی سے آپ جان سکتے ہیں کہ ویب سائٹ پر ہیکنگ کے حملے ہو رہے ہیں۔ حملہ آور بوٹس اور فالتو ہوسٹس کو اس کی مدد سے جانا اور ban یا بلاک کیا جا سکتا ہے تاکہ مستقبل میں ایسے حملوں سے محفوظ رہا جا سکے۔

تھیم کی تدوین

جیسا کہ ہم نے پہلے ذکر کیا کہ ورڈ پریس ایڈمن پینل میں تھیم ایڈیٹنگ کی سہولت موجود ہوتی ہے۔ اگر ہیکر ایڈمن پینل میں لاگ اِن ہو جائے تو وہ تھیم فائل میں تبدیلی کر کے فوراً ویب سائٹ ہیک کر سکتا ہے۔ اس پلگ ان سے تھیم ایڈیٹنگ کی سہولت باآسانی غیر فعال کی جا سکتی ہے۔

غرض اس پلگ اِن میں ورڈ پریس ویب سائٹ کو محفوظ بنانے کا تقریباً سارا سامان موجود ہے اور یہ بالکل مفت بھی دستیاب ہے۔ اگر آپ ورڈ پریس ویب سائٹ رکھتے ہیں یہ ہمیں یقین ہے کہ آپ ضرور اس پلگ اِن کو اپنی ویب سائٹ میں شامل کریں گے اور اگر آپ ایک نئی ورڈ پریس ویب سائٹ بنانے کا سوچ رہے ہیں تو ان تمام باتوں کا خیال رکھ کر آپ ایک انتہائی محفوظ ویب سائٹ تشکیل دے سکتے ہیں۔

ویب سائٹ فائلز اسکین کریں

اگر آپ کی ویب سائٹ خدانخواستہ ہیک یا مال ویئر سے متاثر ہو جائے اور آپ کو مال ویئر کا سراغ نہ مل رہا ہو تو تمام فائلوں کو زِپ کر کے کسی آن لائن اسکینر سے اسکین کریں جیسے کہ وائرس ٹوٹل یا ایواسٹ آن لائن اسکینر۔ ایواسٹ کا اسکینر بھی بہت عمدہ ہے یہ آپ کو بالکل درست مال ویئر زدہ فائل کی نشاندہی کرتا ہے۔

http//:91.213.143.22

اختتامیہ

ورڈ پریس ایک بہترین کانٹینٹ منیجمنٹ سسٹم ہے اور یہ اتنا کمزور بھی نہیں جتنا اس کو تصور کیا جاتا ہے۔ ورڈ پریس بنانے والے اس میں دریافت ہونے والی خامیوں کو بہت جلد ٹھیک کر کے اپ ڈیٹس ریلیز کرتے رہتے ہیں۔ یہ بات اگرچہ کہنے کی ضرورت نہیں لیکن پھر بھی کہنا پڑتی ہے کہ کوشش کریں ہمیشہ ورڈ پریس اور انسٹال پلگ اِنز ہمیشہ اپ ڈیٹڈ رہیں۔ جو تھیمز یا پلگ اِنز استعمال میں نہ ہوں انھیں سرور پر رکھنے کی ضرورت نہیں، انھیں فوراً ڈیلیٹ کر دیا کریں۔

کسی بھی طرح کے نقصان سے بچنے کے لیے ہفتہ وار یا کم از کم ماہانہ کی بنیاد پر ویب سائٹ بمعہ ڈیٹا بیس کا بیک اپ بناتے رہیں۔ جس طرح آپ اپنی دیگر قیمتی چیزوں کی حفاظت کرتے ہیں اسی طرح اپنی ویب سائٹ کو بھی قیمتی سمجھیں اور اس کی حفاظت کے جتنے اقدامات کر سکیں ضرور کریں۔

درج ذیل آسان سوالوں کے جوابات دے کر آپ حاصل کرسکتے ہیں، **2000** روپے تک کا کیش پرائز

1) NoSQL ان میں سے کس کا مخفف ہے؟

☆No Only SQL ☆Not SQL ☆Not Order SQL

2) ان میں سے کونسی امریکی کمپنی **Big Blue** کے نام سے جانی جاتی ہے؟

☆آئی بی ایم ☆مائیکروسافٹ ☆ایپل

3) ان میں سے کونسا آپریٹنگ سسٹم لینکس کی ڈسٹرو نہیں ہے؟

☆Debian ☆RedHat ☆amoebaOS

☆......ان سوالات کے جوابات 15 ستمبر تک ارسال کئے جاسکتے ہیں۔

☆......کوپن پر جوابات لکھ کر اس کوپن کی اسکین کاپی یا موبائل سے فوٹو کھینچ کر بھی بھیجا جاسکتا ہے۔ موصول ہونے والی ای میلز چونکہ بہت زیادہ ہوتی ہیں، اس لئے کوپن مل جانے کی اطلاع دینا ہمارے لئے ممکن نہیں۔

پہلا انعام 2000 روپے نقد	(ایک انعام)
دوسرا انعام 200 روپے نقد	(10 انعامات)

ماہ جون کے سوالات کے درست جوابات

1: پوائنٹ آف سیل   2: پاور پی سی   3: آبجیکٹ اورینٹڈ لینگوئج

پہلا انعام

قیصر نظامی، اسلام آباد

دوسرا انعام جیتنے والے دس قارئین

☆ زبیر احمد، کراچی ☆ عبدالوکیل، شیخوپورہ ☆ جنید، کراچی ☆ ذولقرنین حیدر، حیدرآباد ☆ سہیل خان، پشاور ☆ عاطف بشیر احمد، لاہور ☆ عادل خانزادہ، اسلام آباد ☆ الیاس قادری، کراچی ☆ اظہرالدین، خانیوال ☆ ابوعبداللہ، سکھر

انعامی کوپن برائے ماہ اگست 2014ء

جوابات: 1) .... 2) .... 3) ....

نام .... فون نمبر ....

پتا ....

....

یہ کوپن crm@computingpk.com پر ای میل کیجیے یا ''ماہنامہ کمپیوٹنگ'' پوسٹ باکس نمبر 786، کراچی 74200 پر بذریعہ ڈاک ارسال کیجیے

پلے ڈرون

ایک ریسرچ پروجیکٹ جس نے گوگل پلے اسٹور پر دستیاب ایپلی کیشنز میں سنگین نوعیت کی سکیوریٹی خرابیاں دریافت کیں

اینڈرائیڈ ایپلی کیشنز، گیمز وغیرہ ڈاؤن لوڈ کرنے کے لیے ایک ہی مارکیٹ ذہن میں آتی ہے، گوگل پلے اسٹور (PlayStore)۔ گوگل پلے سے خریداری یا مفت ڈاؤن لوڈ کرنے والا صارف معیاری ایپلی کیشنز کی تلاش میں رہتا ہے تا کہ وہ اسے جلد ڈاؤن لوڈ کر کے حلقہء احباب میں اپنے ذوق کا لوہا منوا سکے۔ گوگل پلے پر کوئی مطلوبہ ایپلی کیشن تلاش کرتے وقت عموماً جس مسئلے کا سامنا رہتا ہے وہ مختلف ناموں سے ایک لے آؤٹ حتیٰ کہ ایک ہی جیسی ایپلی کیشن کا ڈاؤن لوڈ ہوجانا ہے اور یہ بڑا جھنجلا دینے والا تجربہ ہوتا ہے۔ تاہم زیادہ سنگین بات جس کے لیے ہر اسمارٹ فون و ٹیبلیٹ صارف فکر مند رہتا ہے وہ فون کے اندر اور دورانِ استعمال ڈیٹا سکیوریٹی کا ہوتا ہے۔

18 جون کو اے سی ایم سگمیٹرکس (ACM SIGMETRICS) کانفرنس منعقد ہوئی اس کانفرنس کی وجہء شہرت وہاں پیش کیا جانے والا ایک تحقیقی مقالہ تھا جسے اعلیٰ درجے کے کین سیوچک آؤٹ اسٹینڈنگ اسٹوڈنٹ پیپر سے نوازا گیا۔ یہ مقالہ کولمبیا انجینئرنگ کمپیوٹر سائنس کے پروفیسر جیسن نیح (Jason Neih) اور ان کے پی ایچ ڈی کے طالبِ علم نکولس وینوٹ (Nicolas Viennot) اور ایڈورڈ گارسیا (Edward Garcia) نے پیش کیا۔ اس مقالے میں انھوں نے گوگل پلے میں سنگین حفاظتی مسائل دریافت کیے ہیں۔

گوگل پلے، گوگل اینڈرائیڈ کا آفیشل ایپس اسٹور ہے جہاں لاکھوں کی تعداد میں ایپلی کیشنز ڈاؤن لوڈنگ کے لئے دستیاب ہے اور اب تک انہیں مجموعی طور پر اربوں کے تعداد میں ڈاؤن لوڈ کیا جا چکا ہے۔

پروفیسر جیسن نیح جو یونی ورسٹی میں انسٹی ٹیوٹ آف ڈیٹا سائنس اینڈ انجینئرنگ کے سائبر سکیوریٹی کے سینئر رکن بھی ہیں، کہتے ہیں کہ ''گوگل پلے پر ایک ملین سے زائد ایپلی کیشنز موجود ہیں اور اب تک پچاس ارب سے زائد بار مختلف ایپلی کیشنز ڈاؤن لوڈ کی جا چکی ہیں۔ لیکن اب تک کسی نے جائزہ نہیں لیا کہ کیا کچھ گوگل پلے پر اپ لوڈ کیا جا رہا ہے۔ کوئی بھی شخص پچیس ڈالر میں ڈیویلپر اکاؤنٹ حاصل کر کے وہاں جو چاہے اپ لوڈ کر سکتا ہے۔ مجموعی سطح پر وہاں کیا موجود ہے اس بارے میں ابھی بہت کم معلومات موجود ہے۔ گوگل پلے کی مقبولیت اور اس کے کروڑوں صارفین کو لاحق ممکنہ خطرات کو مدِّنظر رکھتے ہوئے ہم نے سوچا کہ گوگل پلے میں موجود اسباب کو قریب سے دیکھنا اہم ہوگا۔''

جیسن نیح اور نکولس وینوٹ کا مقالہ پہلی ایسی تحقیق ہے جس میں گوگل پلے جیسی وسیع مارکیٹ کا بڑے پیمانے پر اور باریک بینی سے تجزیہ کیا گیا ہے۔ یہ کام سر انجام دینے کے لیے انھوں نے پلے ڈرون PlayDrone نامی ایک ایپلی کیشن تیار کی۔ پلے ڈرون ایک ایسا ٹول ہے جو مختلف تکنیکس کو استعمال کرتے

```
public class OAuthUtil
{
  public static final String FACEBOOK_ACCESS_URL = "https://graph.facebook.com/oauth/access_token";
  public static final String FACEBOOK_AUTHORIZE_URL = "https://graph.facebook.com/oauth/authorize?scope=offline_access,read_stream,pu
  public static final String FACEBOOK_CONSUMER_KEY = "6398b84e0cab5449d0b96ee3edaa83cf";
  public static final String FACEBOOK_CONSUMER_SECRET = "70bbded68c14c17b9e1129a6c0754298";
  public static final String FACEBOOK_REDIRECT_URI = "http://www.taptu.com/streams/oauth";
  public static final String GOOGLE_READER_ACCESS_URL = "https://accounts.google.com/o/oauth2/token";
  public static final String GOOGLE_READER_AUTHORIZE_URL = "https://accounts.google.com/o/oauth2/auth?scope=http://www.google.com/rea
  public static final String GOOGLE_READER_CONSUMER_KEY = "67865137267-u52e2pdomdgur3j0v9tq9ihh1cbdvro2.apps.googleusercontent.com";
  public static final String GOOGLE_READER_CONSUMER_SECRET = "6JTT2C99jaXOzwIReZuTugQW";
  public static final String GOOGLE_READER_REDIRECT_URI = "https://www.taptu.com/oauth/google";
  public static final String GPLUS_ACCESS_URL = "https://accounts.google.com/o/oauth2/token";
  public static final String GPLUS_AUTHORIZE_URL = "https://accounts.google.com/o/oauth2/auth?response_type=code&scope=https://www.go
  public static final String GPLUS_CONSUMER_KEY = "843467224689-t71lab1n8tfp5i3ejftf26aa657jontt.apps.googleusercontent.com";
  public static final String GPLUS_CONSUMER_SECRET = "HBIE-XzMz8PD-JDxANqvKLeY";
  public static final String GPLUS_REDIRECT_URI = "http://localhost/";
  public static final String LINKEDIN_ACCESS_URL = "https://api.linkedin.com/uas/oauth/accessToken";
  public static final String LINKEDIN_AUTHORIZE_URL = "https://api.linkedin.com/uas/oauth/authorize";
  public static final String LINKEDIN_CONSUMER_KEY = "loCS0NhUHtflQTgF4_iOD10jSH3zO9tyLSzy_OeEADHpt3VlalmLa_Ylzz_qyG38";
  public static final String LINKEDIN_CONSUMER_SECRET = "vu26Y2K-67b2EBVQYmIpQGfq7soCNhV6dUZgwWj5zRc2IcxZU_vz3xVRvlY1qc4X";
  public static final String LINKEDIN_REQUEST_URL = "https://api.linkedin.com/uas/oauth/requestToken";
  public static final String NETEASEWEIBO_ACCESS_URL = "";
  public static final String NETEASEWEIBO_AUTHORIZE_URL = "";
  public static final String NETEASEWEIBO_CONSUMER_KEY = "rmRqIgt1qznKFA6l";
  public static final String NETEASEWEIBO_CONSUMER_SECRET = "foKTh82TGwEExfI9YfQEfDTJ9ohbV8hf";
  public static final String NETEASEWEIBO_REDIRECT_URI = "http://www.taptu.com/";
  public static final String RENREN_ACCESS_URL = "https://graph.renren.com/oauth/token";
  public static final String RENREN_AUTHORIZE_URL = "https://graph.renren.com/oauth/authorize?scope=read_user_feed read_user_status p
  public static final String RENREN_CONSUMER_KEY = "aa803dbb7b4141ab9da0f6985d353e9c";
  public static final String RENREN_CONSUMER_SECRET = "269de9489344489aae4a0f34fad7c94a";
  public static final String RENREN_REDIRECT_URI = "http://www.taptu.com/";
  public static final String SINAWEIBO_ACCESS_URL = "https://api.weibo.com/oauth2/access_token";
  public static final String SINAWEIBO_AUTHORIZE_URL = "https://api.weibo.com/oauth2/authorize?display=mobile&scope=statuses_to_me_re
  public static final String SINAWEIBO_CONSUMER_KEY = "384815873";
  public static final String SINAWEIBO_CONSUMER_SECRET = "2ac91e387fd7b4995eab65a53d02a654";
  public static final String SINAWEIBO_REDIRECT_URI = "http://www.taptu.com/";
  public static final String TENCENTWEIBO_ACCESS_URL = "https://open.t.qq.com/cgi-bin/oauth2/access_token";
  public static final String TENCENTWEIBO_AUTHORIZE_URL = "https://open.t.qq.com/cgi-bin/oauth2/authorize";
  public static final String TENCENTWEIBO_CONSUMER_KEY = "801253265";
  public static final String TENCENTWEIBO_CONSUMER_SECRET = "b734c468488ae93fbb30bdb3db255d5d";
  public static final String TENCENTWEIBO_REDIRECT_URI = "http://www.taptu.com/";
  public static final String TWITTER_ACCESS_URL = "http://api.twitter.com/oauth/access_token";
  public static final String TWITTER_AUTHORIZE_URL = "https://api.twitter.com/oauth/authorize";
  public static final String TWITTER_CONSUMER_KEY = "m47rQne70ijU7aq6jSjhQ";
  public static final String TWITTER_CONSUMER_SECRET = "HxXXBPjJD8OAXn038HmoT5xuFNxxzXebVxw4oQg9e8";
  public static final String TWITTER_REQUEST_URL = "http://api.twitter.com/oauth/request_token";
```

ہوئے گوگل کے اُس نظام کو ناکام بناتا ہے جو بڑی تعداد میں گوگل پلے اسٹور سے ایپلی کیشنز کو ڈاؤن لوڈ کرنے کے عمل کو روکتا ہے۔ پلے ڈرون نے گوگل پلے اسٹور سے لاکھوں ایپلی کیشنز ڈاؤن لوڈ کیں اور انہیں ڈی کمپائل (decompile) کیا۔ ڈی کمپائل کسی پروگرام کے ایگزی کیوٹ ایبل کوڈ کو واپس سورس کوڈ میں بدلنے کو کہا جاتا ہے۔

ایپلی کیشنز کو ڈاؤن لوڈ کرنے اور انہیں ڈی کمپائل کرنے کے لئے پلے ڈرون کو متعدد سرورز درکار ہوتے ہیں۔ ٹیم نے اپنے تجربے میں دس سرورز کا ایک نیٹ ورک استعمال کیا۔ اب تک پلے ڈرون گوگل پلے اسٹور سے گیارہ لاکھ کے لگ بھگ ایپلی کیشنز ڈاؤن لوڈ کر چکا ہے اور ان میں سے 880,000 ایپلی کیشنز کی ڈی کمپائلیشن کا عمل بھی کامیابی سے مکمل کر چکا ہے۔ ٹیم کے مطابق انہوں نے پلے ڈرون کے ذریعے ڈی کمپائل کئے گئے سورس کوڈ کی 100 ارب لائنوں کا تجزیہ کرلیا ہے۔

ڈی کمپائلیشن سے نیح اور ان کے طلباء کو ایپلی کیشنز کے بارے میں انتہائی اہم معلومات حاصل ہوئیں اور انہوں نے ایک سنگین نوعیت کی خرابی کا پتا چلایا۔ انہوں نے دیکھا کہ ڈیولپرز اکثر اپنے ایپلی کیشن سافٹ ویئر میں خفیہ کلید (Secret Key) کو بغیر کسی حفاظتی انتظام کے، ایپلی کیشن کے سورس کوڈ میں ہی محفوظ کرتے ہیں۔ یاد رہے کہ فیس بک، لنکڈ ان، ایمزون اور اس جیسی دیگر معروف آن لائن سروسز کی APIs (ایپلی کیشن پروگرامنگ انٹرفیس) تک رسائی کے لئے خفیہ کلید اور خفیہ کوڈ کا نظام استعمال کیا جاتا ہے۔ اس خفیہ کلید اور خفیہ کوڈ کے ذریعہ ان آن لائن سروسز سے ڈیٹا حاصل کیا جاسکتا ہے اور ڈیٹا اپ لوڈ بھی کیا جاسکتا ہے۔ لہٰذا ایپلی کیشن کو ڈی کمپائل کر کے کوئی بھی بدنیت شخص خفیہ کلید اور کوڈ تک رسائی حاصل کر کے صارف کو نقصان پہنچا سکتا ہے۔

نیح کا کہنا ہے ''چوٹی کے ڈیولپرز جنھیں گوگل پلے پر بہترین ڈیولپرز نامزد کیا گیا ہے اور ان کی بنائی ہوئی ایپلی کیشنز صارفین میں انتہائی مقبول ہیں، ان کی ایپلی کیشنز میں بھی یہ خامیاں موجود ہیں۔''

وینوئیٹ کہتے ہیں ''ہم گوگل، ایمیزون، فیس بک اور دیگر خدمات فراہم کنندگان کے ساتھ مل کر کام کررہے ہیں۔ اس سے ہم خطرات میں مبتلا صارفین کو پہچانیں گے اور انھیں مطلع کریں گے۔ ساتھ ساتھ ہم گوگل پلے کو اور زیادہ محفوظ بنا سکیں گے۔ گوگل ان مسائل کے لیے اب ہماری تیار کردہ تکنیکس استعمال کررہا ہے جس سے گوگل کو ایپلی کیشنز کو خرابیوں کے لئے اسکین کرنے کی صلاحیت حاصل ہوگئی ہے۔''

اس ضمن میں گوگل نے ڈیولپرز کو پہلے ہی پیغام بھیجنے شروع کر دیئے ہیں کہ وہ اپنی ایپلی کیشنز درست کرلیں اور خفیہ کلیدیں مٹا دیں۔

نیح اور وینوئیٹ کو امید ہے کہ پلے ڈرون، اینڈرائیڈ ایپلی کیشنز کے جدید طرز کے تجزیئے کے لیے بنیاد فراہم کرے گا۔ نیح کا مشاہدہ ہے کہ ''بڑا ڈیٹا مزید اہم ہوتا جارہا ہے اور اس میں سے اینڈرائیڈ ڈیٹا صرف ایک قسم کا دلچسپ ڈیٹا ہے۔ نت نئے طریقوں سے اینڈرائیڈ ایپلی کیشنز کا بڑے پیمانے پر تجزیہ کرنے کے لیے ہمارا کام مرکزی کردار ادا کرے گا۔ اینڈرائیڈ ایپلی کیشنز کو بہتر سمجھنے اور گوگل پلے پر ایپلی کیشنز کے معیار کو بہتر بنانے کے لیے ہم امید کرتے ہیں کہ پلے ڈرون ایک مفید ٹول ثابت ہوگا۔''

تحقیق کے دیگر مشاہدات یہ ظاہر کرتے ہیں کہ گوگل پلے کی تمام مفت ایپلی کیشنز میں سے تقریباً ایک چوتھائی ایپلی کیشنز ایک دوسرے کے کلون یعنی نقل ہیں۔ یہ ایپلی کیشنز مختلف ناموں کے ساتھ گوگل پلے پر پہلے سے موجود ایپلی کیشنز کی نقل ہیں۔ یہ مسئلہ گوگل پلے پرست خریداری کا سبب رہا ہے تاہم اب اس دریافت سے گوگل پلے نے اپنے اس مسئلے کو پہچان لیا ہے۔ مثلاً گوگل دس بہترین ایپلی کیشنز اور دس بدترین ایپلی کیشنز کی فہرست پیش کرتا آرہا ہے جس میں حیران کن طور پر بدترین کی فہرست میں ایک ایسی ایپلی کیشن بھی شامل ہے جسے ایک ملین سے بھی زائد بار ڈاؤن لوڈ کیا جاچکا ہے۔ واضح طور پر یہ مسئلہ ایپلی کیشن کی کلون کی وجہ سے پیش آیا۔

نیح اور ان کی ٹیم نے پلے ڈرون کو ایم آئی ٹی لائسنس کے تحت github پر مفت ڈاؤن لوڈنگ کے لئے بھی پیش کیا ہے تاکہ دیگر لوگ بھی ان کی اس تحقیق سے فائدہ اٹھا سکیں۔ اگر آپ بھی پلے ڈرون کے ساتھ کھیلنا چاہتے ہیں تو اس درج ذیل ربط سے ڈاؤن لوڈ کرسکتے ہیں:

https://github.com/nviennot/playdrone

پی سی DOCTOR

سوال: ہوسٹ گٹر (Hostgator) کی ہوسٹنگ کیسی ہے اوراس کی بینڈوڈتھ اورڈسک اسپیس کے بارے میں آپ کا کیا خیال ہے؟
منیب الرحمان، فیس بک

جواب: آپ نے اپنے سوال میں یہ واضح نہیں کیا کہ آپ ہوسٹ گٹر کے کون سے ہوسٹنگ پیکیج کے بارے میں پوچھ رہے ہیں۔ ہوسٹ گٹر ایک معروف ہوسٹنگ کمپنی ہے جو شیئرڈ ہوسٹنگ سے لے کر ڈیڈی کیٹڈ ہوسٹنگ تک فراہم کررہی ہے۔ ہم فرض کررہے ہیں کہ آپ کا سوال شیئرڈ ہوسٹنگ کے بارے میں ہے۔ ہوسٹ گٹر پر اپنی ویب سائٹس ہوسٹ کرنے والے ویب سائٹ مالکان میں سے بیشتر اس ہوسٹنگ کمپنی کے بارے میں اچھی رائے رکھتے ہیں۔ لیکن یہ ضروری نہیں کہ اگر کسی شخص کی ویب سائٹ ہوسٹ گٹر پر اچھی چل رہی ہے تو آپ کی بھی لازمی اچھی ہی چلے گی۔

ہوسٹ گٹر اور دیگر معروف ہوسٹنگ کمپنیوں کی ہوسٹنگ میں بنیادی طور پر کوئی فرق نہیں ہے۔ یہ سب ہی شیئرڈ ہوسٹنگ فراہم کرنے کے لئے ایک جیسی ہی ٹیکنالوجیز اور انفرااسٹرکچر استعمال کرتی ہیں۔ لہٰذا اگر آپ کی ویب سائٹ کوئی عام بزنس ویب سائٹ ہے جس پر ماہانہ چند ہزار لوگوں کی آمد متوقع ہے تو آپ کسی بھی معروف ہوسٹنگ کمپنی کی شیئرڈ ہوسٹنگ خرید سکتے ہیں۔ تاہم اگر ویب سائٹ پر وزیٹرز کی ایک بڑی تعداد متوقع ہے اور ویب سائٹ بھی بھاری بھرکم ہے تو ہوسٹنگ کمپنی کی Limitation کے بارے میں بغور پڑھ لیں۔ مثال کے طور پر ہوسٹ گٹر کا بے بی شیئرڈ ہوسٹنگ پیکیج پر ایک مخصوص تعداد میں ہی فائلیں اپ لوڈ کرنے کی اجازت ہے۔ جنوری 2014ء کے شمارے میں ہم نے ویب ہوسٹنگ منتخب کرنے کے لئے ایک خصوصی مضمون شائع کیا تھا۔ اس کا مطالعہ آپ کو ویب ہوسٹنگ منتخب کرنے میں انتہائی مدد کرے گا۔

سوال: سر پلیز مجھے کوئی ایسی ویب سائٹ بتائیں جو ڈیٹا اسٹور کرنے کی سروس مفت فراہم کرتی ہے۔ نیز اُس ویب سائٹ پر ڈیٹا پی سی اور موبائل فونز دونوں سے اپ لوڈ اور ڈاؤن لوڈ کیا جاسکتا ہو۔
مزمل خان، فیس بک

جواب: ایسی کئی ویب سائٹس ہیں جو آپ کو درکار سہولت بالکل مفت فراہم کرتی ہیں۔ تاہم چند معروف ویب سائٹس میں گوگل ڈرائیو، ڈراپ باکس، میڈیا فائر اور 4 شیئرڈ شامل ہیں۔ ان تمام ویب سائٹس پر بنیادی اکاؤنٹ بنانا مفت ہے۔ تاہم ہر فائل شیئرنگ ویب سائٹ مختلف مقدار میں مفت اسپیس فراہم کرتی ہے۔ مثلاً گوگل ڈرائیو پر آپ کو پندرہ گیگابائٹس، ڈراپ باکس پر 2 گیگابائٹس، میڈیا فائر 10 گیگابائٹس کی اسٹوریج مفت ملتی ہے۔ تاہم ان میں سے کچھ ویب سائٹس پر آپ مزید اسٹوریج بھی مفت حاصل کرسکتے ہیں۔ اس کے لئے ان ویب سائٹس کو سوشل میڈیا پر شیئر کرنا ہوتا ہے یا اپنے دوستوں کو بھی اس ویب سائٹ پر سائن اپ کرنے کے لئے راغب کرنا ہوتا ہے۔ ڈراپ باکس پر آپ اپنے دوستوں کو سائن اپ کروا کر خود 16 گیگابائٹس تک کی مفت اسپیس حاصل کرسکتے ہیں۔ جبکہ میڈیا فائر پر 20 گیگابائٹس تک کی مفت اسٹوریج اسپیس حاصل کی جاسکتی ہے۔

گوگل ڈرائیو: https://drive.google.com
ڈراپ باکس: http://www.dropbox.com
میڈیا فائر: http://www.mediafire.com
4 شیئرڈ: http://www.4shared.com

ہم نے جن چار فائل شیئرنگ ویب سائٹس کا ذکر کیا ہے، یہ تمام نہ صرف کمپیوٹر پر بلکہ اسمارٹ فونز پر بھی استعمال کی جاسکتی ہیں۔ ان چاروں نے موبائل فونز کے لئے خصوصی اپلی کیشنز بنا رکھی ہیں جنہیں ڈاؤن لوڈ کرکے آپ موبائل فون سے ڈیٹا اپ لوڈ اور ڈاؤن لوڈ کرسکتے ہیں۔

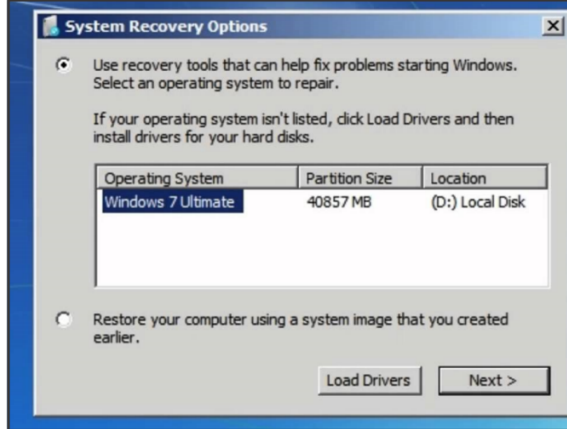
ان فائل شیئرنگ ویب سائٹس کی ڈیسک ٹاپ اپلی کیشنز کے ذریعے آپ خودکار طور پر اپنے کمپیوٹر کا ڈیٹا اپنے اکاؤنٹ میں اپ لوڈ کرسکتے ہیں۔ ان کی ڈیسک ٹاپ اور موبائل فون کی اپلی کیشن میں درجنوں دیگر سہولیات بھی دستیاب ہوتی ہیں۔ مثلاً آپ چاہیں تو ان اپلی کیشنز کو انٹرنیٹ کی دستیاب بینڈوڈتھ کو محدود کرسکتے ہیں تاکہ انٹرنیٹ سے متعلقہ آپ کے دیگر کام متاثر نہ ہوں۔

سوال: میرے کمپیوٹر میں ونڈوز سیون انسٹال ہے جو کہ گزشتہ کافی عرصے سے بغیر کوئی مسئلہ کئے چل رہی تھی۔ لیکن اب اچانک اس نے Bootmgr is missing کا ایرر دینا شروع کردیا ہے۔ اس ایرر کو کیسے دور کیا جاسکتا ہے؟

ضمیر، فیس بک

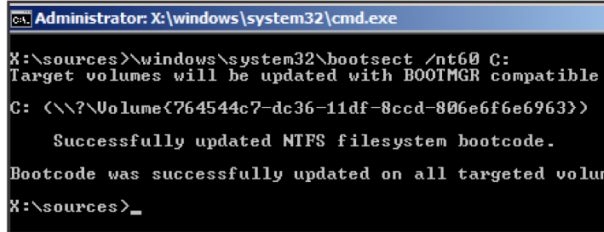
جواب: Bootmgr is missing کا ایرر اس وقت ظاہر ہوتا ہے جب ہارڈ ڈسک پر موجود بوٹ سیکٹر یا تو موجود ہی نہ ہو یا خراب ہوگیا ہو۔ اس مسئلے کو حل کرنے کا سب سے آسان طریقہ تو یہ ہے کہ کمپیوٹر کو ونڈوز سیون کی سی ڈی سے بوٹ کریں اور Install Now کے بٹن پر کلک کرنے کے بجائے Repair your computer کے آپشن پر کلک کریں۔ آپ کے سامنے System Recovery Options کا ڈائیلاگ باکس ظاہر ہوجائے گا۔

```
Administrator: X:\windows\system32\cmd.exe

X:\sources>\windows\system32\bootsect /nt60 C:
Target volumes will be updated with BOOTMGR compatible
C: (\\?\Volume{764544c7-dc36-11df-8ccd-806e6f6e6963})
    Successfully updated NTFS filesystem bootcode.
Bootcode was successfully updated on all targeted volun
X:\sources>_
```

یہاں دو ریڈیو بٹن موجود ہیں۔ آپ پہلا ریڈیو بٹن Use recovery tools... منتخب کیجئے۔ کچھ ہی لمحوں میں اسی ڈائیلاگ باکس میں وہ پارٹیشن ظاہر ہوجائے گی جس میں ونڈوز سیون انسٹال ہے۔ آپ اسے منتخب کرکے Next کے بٹن پر کلک کریں۔ آگے آپ کو کئی ریکوری ٹولز نظر آئیں گے۔ تاہم آپ ان میں سے Startup Repair منتخب کریں۔ کچھ ہی منٹوں میں یہ ہارڈ ڈسک پر موجود بوٹ سیکٹر کو درست کردے گا جس سے ونڈوز دوبارہ بوٹ ہونے کے قابل ہوجائے گی۔

اگر اسٹارٹ اپ ری پیئر کا آپشن بوٹ سیکٹر کو ٹھیک نہ کرپائے تو آپ بوٹ کنفگریشن ڈیٹا (BCD) جو ونڈوز کے بوٹ ہونے میں کلیدی کردار ادا کرتا ہے، کو بذریعہ کمانڈ بھی درست کرسکتے ہیں۔ اس کے لئے ریکوری ٹولز میں سے Command Prompt کا انتخاب کریں اور کمانڈ پرامپٹ پر Bootrec /RebuildBcd ٹائپ کرکے اینٹر کیجئے۔ اس کمانڈ کی وجہ سے بوٹ کنفگریشن ڈیٹا rebuild کرکے پرانے سے بدل دیا جاتا ہے۔ اس سے ونڈوز کے دوبارہ بوٹ ہونے کے امکانات زیادہ روشن ہوجاتے ہیں۔

اگر اس کے باوجود بھی ونڈوز بوٹ ہونے سے منکر ہوجائے تو ایک کوشش مزید کرکے دیکھ لیجئے۔ ریکوری ٹولز میں سے ایک بار پھر کمانڈ پرامپٹ کا انتخاب کریں اور یہاں یہ کمانڈ لکھ کر اینٹر کیجئے:

bootsect /nt60 c:

جب یہ کمانڈ کامیابی سے چل جائے تو اب کمانڈ پرامپٹ پر diskpart کی کمانڈ ٹائپ کرکے اینٹر کردیں۔ diskpart مائیکروسافٹ کی فراہم کردہ ایک کمانڈ لائن ڈسک پارٹیشننگ یوٹیلیٹی ہے جو ونڈوز 2000 سے مائیکروسافٹ ونڈوز کا حصہ ہے۔ اس سے پہلے یہ کام fdisk یوٹیلیٹی سے کیا جاتا تھا۔ خیر، diskpart یوٹیلیٹی کو چلانے کے بعد آپ list disk ٹائپ کرکے اینٹر کریں۔ اس سے آپ کے کمپیوٹر میں نصب ہارڈ ڈرائیوز کی فہرست ظاہر ہوجائے گی۔ ہم فرض کرلیتے ہیں کہ آپ کے کمپیوٹر میں ایک ہی ہارڈ ڈسک نصب ہے۔ لہٰذا اب آپ یہ کمانڈ لکھیں: select disk 0۔ اس کے بعد select partition 1 اور آخر میں active کی کمانڈ ٹائپ کرکے اینٹر کیجئے۔ یہاں نوٹ کیجئے partition 1 سے مراد C ڈرائیو ہے۔

کمانڈ پرامپٹ exit ٹائپ کرکے اینٹر کریں اور کمپیوٹر کو ری اسٹارٹ کردیں۔ امید ہے کہ اس بار ونڈوز کامیابی سے بوٹ ہوجائے گی۔

پاکستان بھر میں کمپیوٹنگ کے ڈسٹری بیوٹرز

شہر	ڈسٹری بیوٹر
کراچی	گلستان نیوز ایجنسی، فریئر مارکیٹ
لاہور	گلزار نیوز ایجنسی، اخبار مارکیٹ
فیصل آباد	ملک افتخار برادرز نیوز ایجنسی، عرفات بزنس سینٹر
ٹوبہ ٹیک سنگھ	جنگ نیوز ایجنسی، نزد ریلوے کراسنگ، کمالیہ روڈ
ملتان	اشفاق نیوز ایجنسی، صمد پلازہ، نواں شہر چوک
راولپنڈی	اشرف نیوز ایجنسی، کمیٹی چوک، اقبال روڈ
پشاور	زرباغ خان نیوز ایجنٹ، چوک یادگار
حیدر آباد	مہران نیوز ایجنسی
رحیم یار خان	چوہدری امانت علی اینڈ سنز
بھکر	عامر نیوز ایجنسی، ریلوے اسٹیشن چوک

* **آزاد کشمیر:** اعظم نیوز ایجنسی، میاں محمد روڈ، میرپور
* **احمد پور ایسٹ:** اسلامی کتب خانہ، نزد گرلز ہائی اسکول، ڈسٹرکٹ بہاول پور
* **احمد پور شرقیہ:** اسلامی کتب خانہ، ضلع بہاولپور
* **اوکاڑہ:** رحمت بک اسٹال، نزد ریلوے پل
* **بنوں:** امیر جان نیوز ایجنسی، چوک بازار، ضلع بنوں
* **بہاولنگر:** دولت خان نیوز ایجنسی، اردو بازار، بہاولنگر
* **پنڈی گھیپ:** پاکستان نیوز ایجنسی، مین بازار
* **تلہ گنگ:** گلوبل کمپیوٹر سینٹر، اولڈ بس اسٹینڈ، ڈسٹرکٹ چکوال
* **تربت:** پاک نیوز ایجنسی، مین روڈ
* **جام شورو:** کامریڈ بک سٹال، ریلوے کراسنگ
* **جھنگ:** شیخ محمد حسین نیوز ایجنٹ، فوارہ چوک، جھنگ صدر
* **جھنگ:** ہمدرد نیوز ایجنسی، رفیقی چوک، شورکوٹ چھاؤنی
* **چشتیاں:** شاہین لائبریری، اُردو بازار، ضلع بہاولنگر
* **چشتیاں:** دولت خان نیوز ایجنسی، اردو بازار
* **چکوال:** حاجی برادرز بک سیلز
* **حاصل پور:** محمد وقاص وحید نیوز ایجنسی، ضلع بہاولپور
* **خانپور:** چوہدری بشیر امانت علی اینڈ برادرز، ریلوے روڈ
* **خانیوال:** طاہر اسٹیشنری مارٹ اینڈ نیوز ایجنسی، کچہری بازار
* **ڈیرہ اسماعیل خان:** قمر بک اسٹال، اردو بازار
* **ڈیرہ غازی خان:** ناصر نیوز ایجنسی، فریدی بازار، ٹریفک چوک
* **رحیم یار خان:** چشتی لائبریری، ابوظہبی روڈ، بلمقابل خواجہ فرید کالج
* **سرگودھا:** پاکستان اسٹینڈرڈ بک ڈپو، بلاک نمبر 10، پھٹہ منڈی روڈ
* **سرگودھا:** پاکستان نیوز ایجنسی، نزد گول چوک، پھٹہ منڈی روڈ
* **سکھر:** الفتح نیوز ایجنسی، مہران مرکز
* **سیالکوٹ:** علمی مرکز، اردو بازار
* **صادق آباد:** چوہدری نیوز ایجنسی، ریلوے روڈ
* **کھاریاں:** شبیر چوہدری، چوہدری نیوز ایجنسی، گلیانہ روڈ
* **کوٹ ادو:** عابد شاپر فروش، بالمقابل بس اسٹینڈ، کوٹ ادو، ضلع مظفر گڑھ
* **کوٹ ادو:** اجمل نیوز ایجنسی، جی ٹی روڈ، کوٹ ادو، ضلع مظفر گڑھ
* **گجرات:** پاکستان بک سروس، 30، اُردو بازار
* **گجرات:** خالد بک ڈپو، مسلم بازار
* **گجر خان:** الفلاح اسلامک نیوز ایجنسی، سکہ
* **گلگت:** نارتھ بکس، مدینہ سپر مارکیٹ
* **مظفر گڑھ:** محمد عبداللطیف بلوچ نیشنل نیوز ایجنسی، قنوان چوک
* **میانوالی:** محمدی نیوز ایجنسی، لاری اڈہ
* **نواب شاہ:** سلیمان برادرز، مسجد روڈ
* **واہ کینٹ:** خوشبو ڈائجسٹ سینٹر اینڈ لائبریری، نواب آباد
* **واہ کینٹ:** حبیب اللہ قمر، میلاد چوک
* **وزیر آباد:** نوید نیوز ایجنسی، ریلوے بکسٹال
* **ہارون آباد:** خالد مسعود بزمی، بزمی انٹر پرائزز، نزد بلدیہ آفس

اگر کمپیوٹنگ آپ کے علاقے میں دستیاب نہیں تو برائے مہربانی ہمیں اس نمبر پر مطلع فرمائیں

0342-2507857